Les Tables rOndes

de **GRAS SAVOYE** en partenariat avec **CPP France**

VENDREDI 6 MARS 2009

Identité & Internet

Usurpation d'identité,
Intrusion dans la vie privée,
Fraude documentaire et numérique :

Fantasme ou réalité ?

Quelle protection pour
nos données personnelles ?

Alias. Le nouvel empire des crimes d'identité
Christophe Naudin, Criminologue
Chercheur au Département de Recherches
sur les Menaces Criminelles Contemporaines à l'Université Paris II
Auteur de Histoire de l'identité individuelle d'hier et de demain.
Editions Ellipses Marketing

Vivre avec les menaces liées à l'utilisation du web : identification et prévention
Stéphane Koch, Consultant et Formateur en Gestion de la Réputation sur Internet
Intelligentzia.net - Switzerland

Usurpation d'identité : un défi mondial. Les réponses juridiques en France et à l'étranger
Myriam Quemener, Magistrat
Parquet général de la Cour d'Appel de Versailles
Auteur d'ouvrages sur la Cybercriminalité

Protection de l'Identité : l'expérience du Royaume-Uni
Michael Lynch, Responsable produit Protection de l'Identité
CPP UK

CNIL : protection, liberté, sécurité
Gwendal Le Grand, Chef du Service de l'expertise informatique
Direction des Affaires juridiques, de l'International et de l'Expertise
CNIL

GRAS SAVOYE cpp Forum ATENA

Gras Savoye
Société de courtage d'assurance et de réassurance
Siège social : 2 à 8, rue Ancelle, BP 129, 92202 Neuilly-sur-Seine Cedex. Tél. 01 41 43 50 00. Télécopie 01 41 43 55 55. http://www.grassavoye.com S.A. au capital de 1 432 600 euros.
311 248 637 R.C.S. Nanterre N° FR 61 311 248 637. Intermédiaire immatriculé à l'ORIAS sous le N° 07 001 707. (http://www.orias.fr).
Sous le contrôle de l'ACAM, Autorité de contrôle des Assurances et Mutuelles, 61 rue Taitbout 75009 Paris.

Les intervenants

Ouverture de séance, Introduction & Conclusion

Marie Bazetoux, Directeur D.I.F.I.D - GRAS SAVOYE

Guy de Felcourt, Directeur Général de CPP France

Alias. Le nouvel empire des crimes d'identité

Christophe Naudin, Criminologue

Chercheur au Département de Recherches sur les Menaces Criminelles Contemporaines à l'Université Paris II

Auteur de *Histoire de l'identité individuelle d'hier et de demain*. Editions Ellipses Marketing

Vivre avec les menaces liées à l'utilisation du web : Identification et prévention

Stéphane Koch, Consultant et Formateur en Gestion de la Réputation sur Internet

Intelligentzia.net - Switzerland

Usurpation d'identité : un défi mondial. Les réponses juridiques en France et à l'étranger

Myriam Quemener, Magistrat

Parquet général de la Cour d'Appel de Versailles

Auteur d'ouvrages sur la Cybercriminalité

Protection de l'Identité : l'expérience du Royaume-Uni

Michael Lynch, Responsable Produit Protection de l'Identité

CPP UK

CNIL : protection, liberté, sécurité

Gwendal Le Grand, Chef du Service de l'expertise informatique

Direction des Affaires juridiques, de l'International et de l'Expertise

CNIL

Marie Bazetoux. C'est avec un grand plaisir que je vous accueille pour cette huitième édition des Tables Rondes de Gras Savoye. Je reconnais certains habitués que je remercie de leur assiduité. J'espère seulement qu'elle n'est pas uniquement due à la qualité des croissants ! Je souhaite que les nouveaux venus deviennent à leur tour des fidèles ; ils manifesteraient ainsi leur intérêt pour ces rencontres.

Les Tables Rondes de Gras Savoye consistent à réunir, autour d'un thème de société, des experts dans des disciplines aussi variées que la philosophie ou la technologie.

Aujourd'hui, notre sujet est : « Identité et Internet ».

Et la question posée est : quelle protection pour nos données personnelles ?

Pour respecter notre tradition, nous nous sommes entourés d'un criminologue analyste de l'identité, d'un as de la cybertechnologie, d'une juriste engagée contre la cybercriminalité et d'un représentant de l'administration publique, défenseur de nos libertés.

Cette huitième édition comporte une particularité : notre partenariat avec CPP, société de services marketing et d'assistance aux consommateurs, qui occupe une position de leader sur le marché britannique et avec laquelle nous étudions l'adaptation au marché français de produits d'assurance et d'assistance dans le domaine de la protection de l'identité.

Je laisse la parole à Guy de Felcourt, directeur général de CPP France, qui introduira notre table ronde.

Je me chargerai ensuite du rôle de modérateur, et veillerai tout particulièrement à ce que le temps réservé au débat soit respecté.

Guy de Felcourt. Au nom du groupe CPP et de Gras Savoye, et en mon nom propre, je vous souhaite également la bienvenue. Pour vous mettre en appétit et pour introduire cette table ronde, je vous rappellerai certains faits survenus ces dernières années.

En Allemagne, 17 millions de clients du groupe Deutsche Telekom ont appris un matin, en lisant le magazine *Der Spiegel*, que leurs données personnelles se trouvaient dans la nature.

En 2008, les associations de consommateurs allemandes ont décidé de faire un test en achetant des données personnelles sur Internet. Pour 850 euros, elles ont récupéré 6 millions de données personnelles, dont 4 millions de données bancaires et financières.

Au Royaume-Uni, également au cours de ces deux dernières années, des millions de données concernant des contribuables et des assurés sociaux ont été égarées. Peut-être me direz-vous que cela pouvait arranger les contribuables !

Toujours au Royaume-Uni, la fraude aux cartes de crédit et la fraude sur les transactions en présence du client ne représentent aujourd'hui plus que 14 % de la fraude totale aux cartes. Voyez l'évolution en la matière !

En France, nous suivons le même chemin. L'observatoire de la sécurité des cartes de paiement a publié des statistiques pour 2007, dans lesquelles il apparaît que les transactions à distance, qui représentent 5 % des transactions par carte, représentent déjà 44 % de la fraude aux cartes. C'est impressionnant !

Toujours en France, rappelons que le compte bancaire du Président de la République a été piraté par de petits escrocs, compte qu'il détient pourtant dans un grand établissement. Si cela arrive au premier des Français, on peut penser que cela peut arriver à chacun des 60 millions de Français.

Aux États-Unis, le phénomène de fraude sur les données personnelles et d'usurpation d'identité a pris une telle ampleur que, en 2007, a été instituée une *task force* présidentielle chargée de coordonner, au niveau fédéral, l'action des huit agences fédérales de lutte contre la fraude aux données personnelles et à l'usurpation d'identité. La présidence a d'ailleurs rendu son premier rapport en 2008.

Ces exemples nous interpellent. Ces phénomènes sont-ils circonscrits, isolés, ou bien correspondent-ils à un mouvement de fond qui toucherait la France et auquel il conviendrait d'accorder la plus grande importance ? C'est l'une des questions que nous aborderons au cours de cette table ronde.

De quoi allons-nous parler aujourd'hui ? Nous allons d'abord parler d'identité. Qu'est-ce que l'identité ? Quelles sont les formes de l'identité ? Comment se traduit notre identité physique lorsqu'il s'agit d'établir une relation à distance avec, par exemple, des institutions financières ? Quelle est la réalité de la fraude identitaire dans notre pays, s'agissant notamment de sa forme la plus visible, à savoir la fraude documentaire ? Quelles sont les évolutions à attendre en la matière ? Je pense par exemple à la biométrie, à la nouvelle carte d'identité électronique, qui a été annoncée par le Gouvernement.

Ensuite, nous parlerons des fraudes par Internet. Quelles sont les menaces spécifiques d'Internet sur les données personnelles ? Le risque est-il réel que notre nom, notre date de naissance ou d'autres données personnelles se retrouvent sur des moteurs de recherche, sur des *blogs*, sur des réseaux sociaux ou socioprofessionnels ? Quels sont les impacts du *phishing*, des failles possibles d'adressage sur Internet ? Enfin, quels sont les impacts de la cybercriminalité ?

Puis nous évoquerons les menaces spécifiques qui pèsent, par le biais d'Internet, sur les cartes bancaires ou les comptes bancaires.

Nous parlerons également de l'évolution des règles et des instruments nationaux et internationaux, des aspects réglementaires et juridiques relatifs à ces questions. Quels sont les projets, en la matière, du Gouvernement ou de l'Union européenne ? Quels rôles peuvent jouer les centrales « antifraude » ou plateformes de signalement telles que FTC/Sentinel aux États-Unis et le CIFAS au Royaume-Uni.

Nous parlerons de la coopération internationale entre les autorités de tutelle ou les entités de régulation. Comment cette coopération se manifeste-t-elle sur ces sujets ? Le G29, qui regroupe les CNIL européennes, a-t-il une vision commune, par exemple, sur le consentement du consommateur à l'égard du traitement de ses données personnelles, sur la finalité de ces traitements ou sur le *modus operandi* des fichiers antifraude ?

Enfin, nous parlerons de la relation entreprises-consommateurs. Comment cette relation est-elle concernée par ces menaces ? Quel est le devoir relatif d'éducation, de conseil, qu'ont les institutions financières ou les opérateurs grand public vis-à-vis des consommateurs ? Comment d'autres marchés, par exemple au Royaume-Uni, ont-ils mis en place une protection des consommateurs dans ces domaines ? Il faut savoir que, dans ce pays, des offres en la matière se sont développées depuis cinq ans.

Pour conclure, nous verrons quels sont les nouveaux services et les nouvelles offres que, en tant qu'institution financière ou opérateur grand public, vous pouvez proposer à vos clients.

Comme vous le voyez, ce programme dense et passionnant est d'une intense actualité. Aussi, sans plus attendre, je passe la parole à Marie, qui va lancer le débat et présenter nos orateurs.

Marie Bazetoux. Je donne la parole à notre premier intervenant, Christophe Naudin, universitaire, chercheur au département de recherche sur les menaces criminelles contemporaines de l'université Panthéon-Assas. Il s'intéresse particulièrement à deux domaines : la sûreté aérienne et la fraude documentaire. Il exerce deux autres activités, et non des moindres : il intervient dans la formation des corps publics, tels que les policiers, et il est l'auteur de différents ouvrages.

Nous avons conservé comme intitulé de sa présentation le titre de l'un de ses ouvrages, à savoir *Alias. Le nouvel empire des crimes d'identité*. Il vient d'en publier un tout récemment intitulé *Histoire de l'identité individuelle. D'hier et de demain*. C'est un livre passionnant, qui se lit comme un roman, et qui présente un panorama des notions d'identité et d'usurpation d'identité à travers les âges.

Son intervention s'inscrit logiquement comme la première de cette matinée. Il dressera les grandes lignes de l'histoire de l'identité individuelle ainsi qu'une typologie de la criminalité identitaire. Je suis certaine qu'il abordera l'un de ses sujets favoris, qui fait débat : quel est le meilleur moyen d'identifier un individu dans l'avenir ?

Christophe Naudin.

(Cf présentation en annexe)

Bonjour, merci de m'accueillir. Il est toujours sympathique de rencontrer des assureurs lorsqu'on n'a aucun sinistre à déclarer ! Je vais tenter de vous intéresser pendant une vingtaine de minutes à la problématique de l'identité.

Les fausses identités sont-elles une altération de l'État de droit ? La réponse est oui. L'usage des fausses identités est de plus en plus répandu ; les fausses identités sont le dénominateur commun à toutes les infractions que l'on connaît aujourd'hui et 80 % d'entre elles ne sont pas détectées aujourd'hui. Cela soulève un certain nombre de problèmes !

Je citerai rapidement quelques exemples tirés de l'actualité récente.

Le mois dernier, M. Poirier, déclaré mort en 2007, a eu un mal fou à être « ressuscité » par le tribunal de grande instance de Paris. C'est une altération du droit civil.

Autre exemple, toujours en droit civil, celui du petit Mohamed, six ans, découvert abandonné dans une cité. Quelqu'un se présente en prétendant être sa mère. Les tests ADN prouvent que tel n'est pas le cas. Mais alors, qui est sa mère ? On ne le sait toujours pas.

Toujours en matière de justice, cet homme que vous connaissez (photo de Dragan Dabic alias Radovan Karadzic – ancien leader des Serbes de Bosnie), a réussi à vivre sous une fausse identité pendant treize ans alors que c'était un criminel de guerre recherché. Nous vivons dans une société de technologies très performantes de l'information ; pourtant, on a mis de nombreuses années années à l'identifier.

Le mois dernier, cet individu, Aribert Heim, un ancien SS qui avait changé d'identité et qui vivait en Egypte sous le nom de Tarek Hussein Farid, a été déclaré mort. On ne sait toujours pas s'il est réellement mort.

En matière de terrorisme, cet homme, basque français ou espagnol, je ne saurais vous dire, a passé sept ans sous une fausse identité au Canada.

Celui-ci, Farid Chalabi, un Français de Saint-Étienne, a vu son identité usurpée sept fois dans le cadre d'un réseau terroriste. Pendant ce temps, M. Chalabi n'a pu obtenir aucun document d'identité parce qu'on ne savait pas si le terroriste, c'était lui ou l'un des six autres.

Les questions d'identité soulèvent donc un réel problème, et ce jusqu'à un niveau politique. Ainsi, aux Pays-Bas, on s'est aperçu qu'Ayaan Hirsi Ali, alors qu'elle était députée, était entrée dans ce pays sous une fausse identité.

Accepter les fausses identités reviendrait à déstabiliser notre système.

Les fraudes à la fausse identité coûtent à la sécurité sociale 1 % de son budget, soit 1,4 milliard d'euros. En 2010, les billets d'avion qui sont utilisés avec une fausse identité coûteront aux compagnies aériennes membres de l'IATA 21 milliards de dollars.

Nous avons aussi le cas d'une femme qui s'était immatriculée auprès de dix-sept caisses d'allocations familiales et qui touchait 22 000 euros par mois pour des quintuplés fictifs.

Le phénomène prend de l'ampleur, à tel point que les cas de fausses identités augmentent de 40 % par an, selon le ministère de l'intérieur, et de 42 % aux États-Unis, soit un doublement en deux ans.

Un chiffre intéressant : en 1998, on n'enregistrait que 36 000 déclarations de perte ou de vol de documents d'identité français ; en 2004, ce chiffre est passé à 527 000. Ces documents ne sont pas volés ou perdus pour tout le monde !

Une petite confidence : beaucoup sont revendus directement par des Français à des étrangers en situation irrégulière, malgré les efforts constants de l'État, de la police, de la gendarmerie, des magistrats, qui se battent en permanence pour résoudre cette situation extrêmement complexe. Cela soulève un problème en particulier pour les faux permis de conduire. Il s'agit véritablement d'un problème de société.

Il en va de même au Royaume-Uni, en Espagne et en Allemagne. La France n'est pas un pays isolé, elle n'est pas responsable de laxisme politique : elle est, dans la société mondiale, comme les autres pays, victime de ce nouveau phénomène apparu voilà quelques années.

Qu'est-ce qu'une fausse identité ? Elle se décompose en quatre incriminations. Tout d'abord, je vais vous parler des personnes morales, car les fausses identités de personnes morales, les fausses entreprises, sont aussi une réalité.

Citons par exemple le cas de Trésor publicité. Un facteur a eu l'idée de détourner des chèques à l'ordre du trésor public, simplement en ajoutant à l'intitulé de cet ordre les lettres « ité ». Il a pu ainsi encaisser pour 6 millions d'euros en chèques.

Deux personnes originaires du Val-d'Oise, Laurent Laluc et Benjamin Silvani, ont eu l'idée de créer une fausse entreprise au moyen de fausses identités. L'un des deux travaillant dans une recette des impôts, il a pu créer de faux avoirs fiscaux, l'un de 5 millions d'euros, l'autre de 8 millions d'euros.

Concernant les personnes physiques, on dénombre quatre incriminations principales.

Premièrement, l'identité virtuelle, partielle ou totale : on invente un nom et on l'utilise. Il ne faut pas confondre avec le pseudonyme, qui est parfaitement légal. Si j'ai envie de m'appeler Johnny Hallyday, je le peux dans la mesure où je le déclare. Là, il s'agit d'utiliser une fausse identité pour tromper quelqu'un. Deuxièmement, l'usurpation d'identité consiste à prendre l'identité de quelqu'un qui est vivant et qui va donc assumer la responsabilité de mes propres actes.

Troisièmement, la substitution d'identité, par exemple dans le cadre des examens, notamment le baccalauréat : je planche sur mon devoir de mathématiques ou je passe une visite médicale à la place de quelqu'un d'autre. Cela arrive souvent dans l'armée ou bien chez les pilotes de ligne ou les conducteurs de train.

Quatrièmement, le vol d'identité, qui est le délit le plus grave et le moins répandu. La personne qui en est victime n'a aucun moyen pour recouvrer ses droits.

Plusieurs personnes, au cours de l'histoire, ont utilisé de fausses identités. Le docteur Petiot, pour se sauver, a utilisé une fausse identité. Klaus Barbie a fui en Bolivie sous le nom de Klaus Altmann. Christophe Rocquencourt a réussi à vendre dans le 7e arrondissement un immeuble entier au nom de quelqu'un d'autre et est presque parvenu à épouser la fille d'un préfet, ce qui n'aurait pas manqué être cocasse. Une certaine Madeleine Morès a usurpé l'identité d'une homonyme afin de percevoir la modeste retraite de cette dernière, au moyen de documents parfaitement véritables, délivrés par l'État, mais dont les mentions étaient totalement fausses. Le chanteur Joey Starr, quant à lui, s'est amusé à conduire très rapidement sa Mercedes en usurpant l'identité d'un homonyme. Conséquence : cette personne a passé trois mois en prison. Enfin, Véronique Courjault a tué au moins trois de ses enfants. Mais qui sont ces enfants ? Ont-ils été déclarés ? Ont-ils une existence légale ? Non, puisqu'ils n'ont jamais été inscrits à l'état civil. Comment un magistrat va-t-il juger cette affaire ? Bien sûr, l'homicide est réel car le cadavre matérialise l'infraction, mais quelle victime va-t-on défendre ?

Vous voyez que l'identité est au cœur d'un problème de société très important. Qu'entend-on par fausses identités et activités criminelles ? Utiliser une fausse identité, c'est beaucoup plus facile que vous ne le pensez. Nous vivons dans une société qui, depuis toujours, est basée sur la confiance. Voilà quelques années, quand naissait un enfant, on allait soi-même le déclarer à l'état civil, sans que personne ne le vît. On affirmait simplement avoir donné naissance à une fille ou à un fils, à qui l'on avait donné tel prénom. L'employé d'état civil le notait. Aujourd'hui, l'employé de l'état civil se rend à l'hôpital pour procéder aux vérifications. Pour autant, dans la mesure où l'on ne sait pas qui est la mère, il est difficile de faire le lien entre celle-ci et l'enfant.

Pourquoi les cas de fausse identité – ou ce que j'appelle la criminalité identitaire – explosent-ils ? Parce que cela rapporte de l'argent ! En matière de stupéfiants, le bénéfice atteint 8 000 milliards de dollars au niveau mondial. La criminalité identitaire, quant à elle, rapporte 7 600 milliards de dollars. Et l'investissement est bien moindre pour produire de faux documents ou pour usurper l'identité de quelqu'un. En revanche, le trafic de stupéfiants est dangereux, on peut se faire tuer ; en outre, il nécessite une avance de fonds considérable et requiert des distributeurs. C'est très compliqué.

Les premières victimes en matière de criminalité identitaire, ce sont les collectivités, l'État, les caisses d'allocations familiales, les grandes entreprises. Les cas des personnes physiques ne sont pas forcément ceux qui nous marquent le plus. Les cas d'usurpation d'identité sont majoritairement liés aux affaires d'immigration clandestine et de détournements de fonds.

Auparavant, il fallait des « hommes de paille » ; maintenant, il est beaucoup plus facile d'usurper une identité, d'ouvrir un compte ou de créer une société sous un faux nom, faute de vérification de la part du greffe du tribunal.

La prostitution est, elle aussi, concernée : il est toujours plus pratique de se prostituer sous un faux nom.

En matière de terrorisme, contrairement à ce qu'on pourrait penser compte tenu des questions basque et corse, l'usurpation d'identité est, d'une manière générale, moins répandue.

Enfin, les petits trafiquants de toute sorte recourent eux aussi à de fausses identités.

Comment peut-on lutter contre la criminalité identitaire ? Pour répondre à cette question, il faut répondre à une autre question : l'identité est-elle universelle ? Avons-nous tous la même forme d'identité ? Avons-nous tous un patronyme, c'est-à-dire un nom qui nous a été transmis par notre père ?

Premier problème, l'identité, aujourd'hui, est écrite. Notre identité, c'est un bout de papier. Sauf que dans le monde, il existe actuellement cinquante écritures et quinze calendriers différents. Mettez-vous à la place d'un policier aux frontières ! Et puis il existe des cultures nominatives très différentes les unes des autres. Dans la culture arabe, il existe cinq noms différents. Par exemple, cet homme (photo d'Oussama Ben Laden) possède 19 identités. La CIA peut toujours essayer de le chercher ! Il lui faut d'abord trouver son nom véritable. En France, si l'on recherche un voleur de Mobylette, la recherche portera sur un seul nom.

Regardez cette carte : toutes les zones en bleu représentent l'identité sous la forme de celle que l'on connaît aujourd'hui, c'est-à-dire la nôtre : le nom, le prénom et la date de naissance. Tout ce qui est d'une autre couleur représente les autres formes d'identité. Mais si l'on regarde une carte anamorphique, on constate que les couleurs bleues sont très peu représentées. Et il faut savoir qu'en 2050 elles seront encore moins représentées. Cela signifie que notre forme d'identité est en train de disparaître. Cela soulève un gros problème.

Existe-t-il des risques d'homonymie dans le monde ? Regardons de nouveau la carte, plus c'est rouge, plus les risques sont importants. En Europe, il existe 500 000 noms pour 70 millions d'individus. En Chine, pour 1 350 000 000 individus, on compte 1200 noms. En Corée, trois noms de clan sont utilisés par 45 % de la population.

Dans le cadre de vos recherches en matière d'assurance, vous devez réfléchir à la manière de prendre en compte l'ensemble de ces problématiques. Vous connaissez le modèle européen :

un ou plusieurs prénoms, le patronyme, le sexe. Mais le sexe change ! Ce que le législateur n'avait pas prévu à l'origine. Ce modèle-là est très récent : il n'a que 300 ans.

Comment procède-t-on avec un voleur de voitures qui porte tel ou tel nom ? On va translittérer son nom, ce qui n'est pas simple. Selon que l'on est en France, en Allemagne ou au Royaume-Uni, la translittération du nom s'effectuera de manière différente. De surcroît, un nom peut s'écrire différemment dans sa propre langue d'origine. Voyez tous ces calendriers qui ont actuellement cours ! À Roissy, endroit que je connais bien, les policiers aux frontières s'y perdent totalement entre toutes ces dates. Voici un exemple, celui de cet Éthiopien, né le 21 novembre 1979, ou, dans le calendrier éthiopien, le 12 du mois de Hedar 1971. Personne ne verra la différence à Roissy, croyez-le bien. En outre, il existe quatre possibilités pour translittérer son nom et quatre autres pour translittérer son prénom. Cela fait en tout seize identités possibles. Et si je multiplie ce chiffre par deux pour tenir compte de ses deux dates de naissance possibles, il peut potentiellement prétendre à trente-deux identités possibles.

Je vous ai parlé des concepts identitaires. En Mongolie, par exemple, le jour de la naissance correspond au premier anniversaire. Quand, après avoir arrêté un Comorien, situation que j'ai vécue moi-même, vous lui demandez comment il s'appelle, il vous répondra par exemple « Saïd ». Quand vous lui demandez son prénom, il vous répond aussi « Saïd ». Comment s'appelle son père ? Il s'appelle lui aussi Saïd, puisque lui-même s'appelle Saïd. Les policiers aux frontières s'arrachent les cheveux !

Il existe deux types de documents : les vrais faux, c'est-à-dire ceux qui ont été fabriqués dans une quelconque arrière-boutique, et les faux vrais, c'est-à-dire ceux qui ont été délivrés par l'autorité légitime. Pour sécuriser les documents, on a inventé des signes de sécurité, les lettres anamorphiques, qui apparaissent par traitement aux rayons ultraviolets. Mais tous les faussaires savent que, avec de la crème solaire indice 50, on parvient au même résultat ! On a aussi doté les documents de petits points permettant de les identifier. À cet égard, notre passeport est assez bien conçu, mais certains arrivent à découdre la partie centrale pour changer les pages sur lesquelles sont portées des mentions variables. Il existe aussi des pays, tels l'Irak ou l'Afghanistan, où sont vendus des documents totalement fantaisistes. Voyez cette carte, qui fait référence à la « confédération française ». À ma connaissance, la France n'est pas encore une confédération ! S'agissant des permis de conduire, voyez celui-ci : il y est indiqué qu'il a été délivré en 1993.

Sauf que la souche sur laquelle est imprimé ce permis n'a été mise en service qu'en 1999 ! Ainsi, son détenteur avait six ans d'avance sur l'administration !

Il existe aussi un ensemble de procédés visant à altérer les documents. Sur celui-ci ont été grattées certaines mentions, remplacées par d'autres. Sur celui-là, les numéros ont été transformés de manière à modifier la date de naissance. Sur ce dernier, enfin, le film de sécurité a été découpé afin de permettre la substitution de la photo. Ce travail de précision coûte de l'argent. L'ingéniosité des faussaires est sans limite. Autre méthode : inventer un nouveau pays. Ainsi, on compte 10 000 personnes habitant le Sealand. Sur ces 10 000 personnes, 5 000 sont porteurs d'un passeport diplomatique !

Pour combattre ces faux documents, on va essayer de définir ce qu'on appelle l'identité absolue, c'est-à-dire définir un système en vertu duquel notre identité sera attestée non pas par nos papiers, mais par nous-mêmes. Comment va-t-on procéder ? On va se baser sur un dispositif dont sont dotés aussi bien les animaux que les hommes, à savoir la perception qu'on a de son identité quand on rentre chez soi. Personne, avant d'embrasser sa femme ou ses enfants, ne leur demande leur carte d'identité. Pour les identifier, on se base sur une combinaison de sens. En France, nous utilisons les empreintes digitales pour nous identifier les uns des autres, mais c'est un palliatif. Une autre méthode « naturelle » consiste à mesurer en trois dimensions les éléments de la main. On pourrait également mesurer l'oreille, mais ce n'est pas très pratique : les gens n'apprécieraient probablement pas d'apposer leur oreille sur une machine de contrôle. On peut aussi mesurer les petits canaux qui irriguent l'iris, qui sont un marqueur extrêmement puissant de l'identité. Mais cette méthode étant extrêmement intrusive, les gens ne l'apprécient pas. Évidemment, il y a aussi l'ADN. Mais il faut savoir que deux jumeaux homozygotes disposent du même ADN. D'où la nécessité de trouver une méthode qui puisse s'appliquer à tout le monde, sans exception. La solution pourrait consister en une combinaison de ces différentes méthodes. C'est ce qui se passera demain. Nous disposerons d'une carte d'identité biométrique basée non plus sur un seul facteur, mais sur plusieurs facteurs. Ce sera la seule façon d'identifier et de discriminer 20 milliards d'individus dans le monde.

Le débat reste cependant ouvert. Je vous remercie de votre attention.

Marie Bazetoux. Tout cela n'est guère rassurant !

Je vous propose de poursuivre avec Stéphane Koch, qui est le praticien. Le cœur de son métier, c'est l'information. Il conseille et accompagne les entreprises dans le domaine de la gestion de la réputation, de la veille stratégique et concurrentielle en pratiquant ce qu'on appelle l'intelligence économique. Il est aussi formateur et expert en lutte contre la criminalité économique pour divers instituts et universités en Suisse.

Stéphane Koch abordera ici l'aspect identification et prévention des risques. Il est celui qui va nous faire prendre conscience de tous les dangers qui se cachent derrière notre boîte mail et les outils préférés de nos enfants. Il est aussi celui qui va nous faire peur avec des cas concrets. Nous allons enfin comprendre ce qui se passe derrière la toile et aborder un aspect souvent ignoré mais ô combien grave : la détresse des victimes. Je suis certaine qu'il nous livrera aussi des « trucs » pour prévenir les risques que nous courons.

Stéphane Koch.

(Cf présentation en annexe)

Cela fait beaucoup de points à aborder en trente minutes !

Comment le net va-t-il vous voler votre identité ?

Avant toute chose, je lance un appel : je crois que 52 000 clients de l'UBS cherchent par tous les moyens à changer d'identité en ce moment !

L'identité numérique se définit par différents éléments : les informations qu'on a mises en ligne pour créer sa présence ; tous les lieux où l'on est présent, tels les réseaux sociaux, les *webmails*, les sites web, les *blogs* ; parfois l'information produite par les tiers, autorisée ou non ; enfin, les homonymes. Si l'un de vos homonymes a été condamné pour meurtre, il n'est pas forcément très réjouissant de voir votre nom confondu avec le sien lorsqu'on lance une requête sur Google.

Tous ces éléments vont créer une sorte de clone numérique, un Frankenstein numérique à partir d'informations éparses qui constitueront l'identité de la personne sur Internet. En conséquence, tous les éléments constitutifs d'une identité numérique ne sont pas maîtrisables par son détenteur légitime. Aujourd'hui, c'est un problème qui est loin d'être résolu.

Quel est l'état des lieux sur le *web* en matière d'usurpation d'identité ? Si vous ne savez pas comment faire, vous pouvez toujours suivre des cours ! Comment cracker un compte utilisateur, pirater un compte MSN, pirater Facebook, etc… : le tutorat est possible sur Youtube.

L'état de la connaissance est en constante évolution sur Internet. Les choses qui sont censées être protégées, peuvent être défaites selon le principe que ce que l'homme a fait, l'homme peut le défaire. Il existe réellement un marché *business to business* du crime organisé sur Internet. On peut acheter massivement des comptes d'utilisateur, c'est-à-dire que, pour un certain montant, vous pouvez obtenir une certaine quantité de données à exploiter, qu'il s'agisse de comptes sur des réseaux sociaux, de numéros de carte de crédit, etc. Le développement des réseaux sociaux a rendu plus aiguë cette problématique.

La réalité, c'est que des gens se sont effectivement fait voler leur identité sur Facebook. Peut-être me direz-vous que ce n'est pas grave. Sauf que des demandes de rançon ou d'argent ont été formulées par le biais des comptes piratés auprès des personnes – les « amis » – avec lesquelles le titulaire du compte était en contact. Des gens ont reçu un message par lequel un faux ami leur demandait de lui envoyer de l'argent par Western Union. Ainsi, les conséquences peuvent être importantes !

Ou alors, des gens publient une information en se faisant passer pour la personne dont ils ont piraté le compte. Ce genre d'information peut avoir un impact extrêmement préjudiciable à divers égards.

Aux États-Unis, il existe un site recensant tous les cas connus de perte ou de vol de données, d'usurpation potentielle d'identité. Il serait intéressant d'avoir le même système en Europe. Chaque jour un nouveau cas est identifié. Aujourd'hui, compte tenu de la vitesse à laquelle l'information circule, sachant que les éléments techniques qui agissent en interaction avec les facteurs humains ne sont pas toujours maîtrisés, une masse croissante de données sont disponibles de manière non volontaire. Et toutes ces données trouvées ou usurpées peuvent être utilisées à des fins frauduleuses.

Notre propre vie peut être exposée sur Internet. Vous avez certainement entendu parler de ce journal qui s'est amusé à retracer la vie de quelqu'un en utilisant les différents moteurs de recherche disponibles sur Internet. La personne dont il a ainsi retracé la vie a été extrêmement affectée par cette initiative, qui a rencontré un certain écho médiatique. Cela a changé sa vie. Les conséquences d'une usurpation d'identité peuvent être extrêmement préjudiciables. On peut commettre des délits au moyen de cette fausse identité ou en exploitant des failles

technologiques. Par exemple, si vous parvenez à cracker un téléphone mobile et à utiliser le protocole Bluetooth, vous pouvez téléphoner en utilisant le téléphone d'un tiers et, par exemple, lancer une alerte à la bombe à l'aéroport de Roissy. Et le téléphone qui sera identifié sera celui de la personne qui aura subi le piratage.

La multiplication des homonymes soulève aussi un problème. Sur Facebook, rien qu'en Suisse, il existe plus d'une centaine de Jean Dupont. Il s'agit sans doute chaque fois d'un vrai Jean Dupont. On n'en sait rien. On pourrait aller voir les amis de chacun de ces Jean Dupont et essayer de croiser les informations…

Je me suis amusé à identifier l'entreprise pour laquelle j'interviens aujourd'hui. Je me suis demandé quelles informations je pourrais trouver sur les gens qui la composent ; pourrais-je envisager d'utiliser les identités ou de me les approprier d'une manière ou d'une autre ? Sur Linkedin, qui est un réseau professionnel, j'obtiens environ 218 résultats. Sur Viadeo, j'en obtiens 700. Je peux ainsi obtenir des informations intéressantes à différents niveaux et mieux percevoir la nature de ma cible. Une fois que j'ai ces informations grâce à tel ou tel site, je peux accéder à différentes catégories de personnes exerçant des responsabilités. Ensuite, sur des sites tels que Kompass, vous obtiendrez là encore d'autres informations. Vous pouvez aussi y acheter des rapports exhaustifs, si vous le désirez. Vous disposez aussi de sites tels que celui du *Who's who in France* ou Facebook, sur lesquels vous pouvez aussi obtenir des informations.

Ainsi, on peut croiser les réseaux sociaux, les informations, pour dresser une sorte de profilage de l'identité. À partir de cela, on peut tout à fait créer des identités sur des réseaux où ces personnes ne sont pas encore présentes. On va trouver où est le maillon faible pour aller justement usurper cette identité. Par exemple, Facebook compte environ 8 millions d'inscrits en France (chiffres fournis par le site). Cela permet d'identifier parfois les employés d'une entreprise.

Ainsi, afin de déterminer le nombre de salariés de Gras Savoye inscrits sur ce site, j'ai créé un faux compte sur le réseau français et j'ai ensuite essayé d'identifier le nombre de personnes qui étaient disponibles.

Ce que j'ai fait là, j'aurais pu le faire sur n'importe quel autre réseau. De fait, ces réseaux ne sont pas bien protégés. Quand vous tapez votre nom d'utilisateur et votre mot de passe, généralement la page n'est pas sécurisée. Si vous vous connectez à partir d'un cybercafé ou d'un réseau sans fil, vos données peuvent être usurpées, votre identité peut être usurpée, et vous perdez de facto la possibilité de vous reconnecter à votre compte.

Je connais plusieurs personnes à qui cette mésaventure est arrivée : subitement, elles n'ont plus eu accès à leur compte, cependant que quelqu'un d'autre avait pris leur place vis-à-vis de leur cercle d'amis.

Donc, je me suis inscrit sur le site français, sur lequel environ 418 employés actuels ou anciens ont mentionné le nom de leur entreprise. Sur ces *slides*, j'aurais pu masquer les noms, mais je ne l'ai pas fait, car il s'agit d'informations publiques. Je n'ai eu recours à aucune astuce pour les obtenir. Elles ne sont pas protégées et sont accessibles à tout un chacun. J'ai simplement dû créer un profil sur le site français, car, de mon profil suisse, je n'avais pas accès aux informations que je voulais obtenir. Mais ces informations, je le répète, sont totalement publiques.

Une fois que les employés potentiels ont été identifiés, on peut croiser les informations avec les noms des responsables, on peut jouer sur les différentes succursales pour se faire de nouveaux « amis ». Je crée le profil d'un dirigeant, par exemple celui de la succursale suisse. Celui-ci n'étant pas forcément connu, je vais commencer par me constituer un cercle d'« amis », puis je vais aller sur d'autres sites et collecter de l'information auprès de cercles qui me considèrent comme digne de confiance. Par exemple, sur Facebook, certains créent un faux profil de *people*, avec qui les véritables amis de celui-ci, croyant qu'il s'agit de la bonne personne, se lient et échangent des informations, des photos, que cet usurpateur n'aurait pas obtenues autrement.

Ce problème d'usurpation d'identité sur Internet est multidimensionnel. Sur les réseaux sociaux, je peux créer un groupe et une page d'entreprise pour ensuite collecter de l'information. Je peux aussi envoyer des courriels piégés sur les messageries des cibles potentielles : une fois que j'ai collecté mon information, une fois que j'ai identifié ou hiérarchisé les responsabilités, je peux adresser un courriel avec un programme intégré. Je vous signale que la plupart des programmes faits main ne sont pas détectables par les systèmes de sécurité. Ils passent comme une lettre à la poste !

Après, je peux exploiter les informations que j'ai recueillies.

La construction de la fraude est extraordinairement facilitée par la possibilité de collecter des informations sur Internet.

Certains vont utiliser Google au moyen de quelques critères, cependant que d'autres auront recours aux opérateurs avancés. C'est toute la différence liée à la connaissance.

Personnellement, peut-être serais-je en mesure de disposer d'autres critères pour savoir si la personne avec laquelle je communique est réellement celle qu'elle prétend être.

De multiples sources sont disponibles : grâce à Google, je peux retrouver les amis de la personne qui possède un compte sur Facebook en récupérant les informations disponibles sur ce site, informations que je peux mémoriser.

La plupart des gens, lorsqu'ils configurent leur profil sur Facebook, ne vont pas veiller à interdire l'accès à certaines des informations qu'il contient. Ils ne s'interrogent pas sur les données qu'ils vont choisir de rendre publiques et sur la manière dont un tiers pourrait utiliser celles-ci de manière inappropriée. Cela étant, c'est bien normal, car on ne peut pas scénariser toutes les possibilités d'une utilisation frauduleuse d'informations qu'on a mises en ligne.

Nous avons parlé de problèmes techniques. Un autre problème est celui de la surface du Web. Facebook compte aujourd'hui 175 millions d'utilisateurs dans le monde. C'est véritablement un phénomène de société : c'est le premier réseau social qui a vraiment rendu beaucoup plus floue, moins perceptible, la différence entre la société réelle et la société virtuelle. Aujourd'hui, on trouve sur ce site des gens qui ne sont pas des fans d'Internet ; ce sont des gens qui n'ont rien à faire sur Internet, qui sont sur ce site uniquement pour ce qu'il leur apporte, c'est-à-dire la capacité de partager des informations. Forcément, le vol des données personnelles et les usurpations d'identité explosent en raison de la facilité d'utilisation de ces outils. Les gens ne sont pas conscients de la face sombre d'Internet, de la manière dont on peut frauduleusement utiliser des identités.

Ces dernières années, trois failles majeures de sécurité sont apparues en matière d'identification.

Lorsque vous consultez un site bancaire, la mention « https » apparaît dans l'URL de votre banque. Ce protocole SSL, qui garantit la confidentialité de l'information que vous transmettez, avait été cracké en 2003. Le problème a été résolu depuis lors.

En 2008, une autre faille de sécurité a été détectée dans le système des noms de domaine. Cette faille permettait plus que le *phishing*. Je rappelle que le *phishing* consiste à tromper sur l'identité d'un site en adoptant la ligne graphique d'un autre site. Le *farming* consiste quant à lui à s'approprier le nom de domaine d'un site connu. Il n'existe aucun moyen direct de constater ce genre de fraude. L'utilisateur normal n'est pas en mesure d'identifier une telle problématique.

La dernière faille de sécurité a été découverte le 30 décembre 2008 et porte sur les certificats numériques associés aux sites.

Lorsqu'un site dispose d'un système de sécurité, on peut lui associer une sorte de carte d'identité numérique. Grâce à cette faille, il était possible de tromper cette carte d'identité numérique en la remplaçant par une fausse carte d'identité.

Donc Internet soulève à la fois une problématique humaine, c'est-à-dire la capacité pour chacun d'y intervenir *via* les réseaux sociaux, mais aussi une problématique technique, qui n'est pas davantage réglée, comme l'attestent les phénomènes de *phishing,* de *farming* et de *botnet* – le terme *botnet* désigne un ensemble d'ordinateurs individuels mal protégés qui, détournés par des outils automatiques, exécutent toutes sortes de tâches malveillantes, par exemple l'envoi de spams, l'attaque de sites, etc. Ainsi, l'Estonie a vu son système Internet bloqué pendant deux jours par des attaques de ce type.

Le réseau sans fil, quant à lui, est peu ou pas protégé. Il est peu protégé si vous avez une clé *web* identifiée sur votre routeur sans fil. Une protection *wep* ne suffit pas. Aujourd'hui, les outils permettant de cracker ces réseaux sont tous disponibles en ligne : on peut casser une clé, se l'approprier et filtrer l'information. Je vous rappelle que toute information qui transite par un réseau est visible si elle n'est pas chiffrée. Si vous vous connectez à votre compte bancaire en dehors du protocole *https*, les informations que vous transmettez sont lisibles par quiconque a accès à ces paquets de données.

De même, quand on perd un téléphone mobile, on perd aussi un carnet d'adresses et toutes sortes d'informations. Certains téléphones mobiles ont une mémoire de 32 gigaoctets. De même, quand on perd son agenda électronique, dont les données ne sont pas chiffrées, on perd une partie d'un patrimoine d'informations. Dernièrement, en Suisse, un médecin avait oublié son ordinateur dans sa voiture, lequel a été volé. Il contenait le dossier de plus de 2 000 patients. Ce médecin étant un chirurgien esthétique, son voleur, s'il avait eu de mauvaises intentions, aurait pu publier un certain nombre de photos sur Internet. Ce médecin a offert une récompense de 4 000 euros à celui qui lui rapporterait son matériel. C'est vous dire s'il était désemparé !

Ce n'est pas parce que vous effacez des données d'un support magnétique que celles-ci disparaissent. C'est un peu comme si vous supprimiez l'adresse de votre domicile de l'annuaire téléphonique : votre domicile existe toujours, même si son adresse n'est plus mentionnée dans l'annuaire. Avec les outils appropriés, il est parfaitement possible de récupérer cette information et de la réutiliser.

Ainsi, outre les risques d'usurpation d'identité, de fraudes, de perte de réputation, de ruptures de contrat, de préjudices économiques ou de chantage, il faut encore envisager les traces négatives qui subsistent de manière indélébile dans les moteurs de recherche. Une fois que votre nom est associé à quelque chose, il est difficile de faire machine arrière. N'allez pas croire que l'on peut tout retirer d'Internet : ce n'est pas vrai. On peut intervenir sur certaines informations, tandis que d'autres resteront éternellement. Le problème d'Internet, c'est qu'il est intemporel. Il réagit à des mots-clés, peu importe que l'information ait cinq ou dix ans d'ancienneté. Il faut vraiment prendre en compte cet aspect des choses. Et puis Internet peut aussi servir à influencer d'autres personnes : ami, collègues, employés, etc. Ces risques, dont la liste n'est pas exhaustive, sont majeurs et sont liés à l'usurpation d'identité.

« Pour un mot, un homme est réputé sage ; pour un mot, un homme est jugé sot », disait Confucius.

Vous remerciant de votre attention, je vous laisse méditer ces paroles.

Marie Bazetoux. Je vous avais dit que cela ne s'arrangerait pas et je ne vous avais pas menti ! Non seulement nos permis de conduire ont été volés, mais encore on ne sait pas ce qu'il va advenir de l'identité de nos enfants qui se sont inscrits sur Facebook.

Pour nous rassurer, nous avons à notre table Myriam Quemener, qui est magistrat au parquet général de la cour d'appel de Versailles, après avoir précédemment occupé un poste de direction au ministère de la justice. Elle est aussi expert pour le Conseil de l'Europe en matière de cybercriminalité et elle participe à des séminaires internationaux sur cette délinquance planétaire. Elle a publié très récemment « *Cybermenaces, entreprises et internautes* » et fin mars sortira la 2ème édition de « *Cybercriminalité. Défi mondial* » écrit avec Joël Ferry, aux éditions Economica.

Au cours de son intervention, elle nous fera découvrir que la cybercriminalité n'a rien de virtuel et qu'elle est le fait d'une délinquance très organisée est très efficace. Nous découvrirons que c'est un monde en soi, qui possède ses codes, son vocabulaire et son organisation.

Elle dressera un panorama des réponses juridiques, tant en France qu'à l'étranger. Elle nous fera partager la mise en œuvre concrète et pertinente de la loi pénale.

Myriam Quéméner. Je remercie Gras Savoye et CPP France de m'avoir invitée à cette matinée passionnante.

Effectivement, après les deux premières interventions, l'angoisse va encore s'accroître puisque je vais vous parler des réponses juridiques qui sont apportées à ce phénomène. En tant que magistrat, je vous ferai part de mon expérience de la justice au quotidien. Comment l'institution judiciaire doit-elle répondre à ce défi qu'est la cybercriminalité, délinquance de demain ? Cela a été dit, cette délinquance peut se répandre très facilement, avec un faible investissement. En outre, elle est moins risquée que ne le sont les braquages. La motivation principale des délinquants, c'est bien sûr l'appât du gain. Cela peut en effet rapporter gros avec un faible investissement.

Cette forme de délinquance est au cœur d'enjeux très importants, qui touchent à la fois la protection de l'ordre public, la protection de la société et, également, la protection des libertés individuelles. Face à Internet et aux réseaux numériques, 71 % des Français estiment qu'ils sont mal protégés.

L'usurpation d'identité est au cœur de nos réflexions. Parmi la liste des attaques, c'est ce qui vient en premier lieu. L'usurpation d'identité est une infraction classique qui existe depuis la nuit des temps. Aux audiences de la cour d'assises, la plupart de mes « clients » utilisent des alias – terme qui signifie « l'autre ». Les accusés essayent de brouiller les pistes, de fuir la justice, et ce phénomène est simplement démultiplié avec Internet et les réseaux numériques.

Qu'est-ce que l'usurpation d'identité ? Cela consiste à prendre délibérément l'identité d'un autre dans le but de réaliser une action frauduleuse, par exemple accéder aux finances de la personne dont on a usurpé l'identité ou commettre un délit ou un crime de façon anonyme, de façon masquée, de manière à échapper à ses responsabilités.

Le recours à Internet et aux réseaux numériques nous rend plus vulnérables face à ce phénomène. La captation frauduleuse est rarement une fin en soi ; elle va permettre de commettre d'autres infractions. Comment cela se traduit-il juridiquement ?

Aujourd'hui, aucune autorité publique ne contrôle l'identité numérique, contrairement à ce qui prévaut en matière d'état civil, lequel est strictement réglementé. En fait, les individus peuvent utiliser un pseudo, différentes identités, se faire passer pour un autre, et il n'existe pas, en l'état, une limite juridique ou technique à la création d'adresses. L'adresse de chaque machine connectée au réseau, à savoir l'adresse IP, est aléatoire et permet d'identifier non pas directement un internaute, mais seulement une machine.

On passe en fait de la notion d'identité, qui est à peu près cadrée – je suis davantage une pénaliste, mais, au regard du droit civil, l'identité d'une personne est une notion établie – à la notion plus complexe d'identité numérique, qui peut être le nom d'utilisateur, le mot de passe, l'adresse URL, l'adresse IP, le numéro de carte bancaire. Tous ces éléments sont regroupés sous le terme « identifiant identité numérique ».

On parle maintenant de « cyber-usurpation » d'identité, phénomène qui s'est amplifié. On parle aussi d'identité jetable, pour reprendre les termes d'un avocat, Maitre Itéanu, qui a publié dernièrement un ouvrage très intéressant sur ce sujet. Les pistes sont brouillées et il est vrai que la justice, comme les services d'enquête, est souvent mise en difficulté. D'où la nécessité de spécialiser les officiers de police judiciaire. En tant que magistrats, nous allons devoir nous spécialiser dans ces domaines. En matière de propriété intellectuelle, il est de plus en plus question de pôles de compétences. Il est nécessaire de regrouper les procédures. Je vous dirai d'ailleurs quelques mots des problématiques en matière de compétence territoriale, qui ne sont plus adaptées à la situation actuelle.

On parle de souveraineté de l'État, de compétence territoriale des tribunaux de grande instance et des cours d'appel. Or la cybercriminalité est mondiale. Un décalage s'est créé, alors que des réponses coordonnées s'imposent au niveau européen et au niveau mondial.

La fraude que permet l'usurpation d'identité s'inscrit dans un processus de délinquance de plus en plus structuré et organisé. On a parlé tout à l'heure de criminalité organisée. Certains pays se sont spécialisés. Voilà quelques mois, j'ai pu consulter la carte d'un pays de l'Est mentionnant les spécialités locales en la matière. Dans certaines régions s'était développée la vente de kits de *phishing* en ligne. Un véritable marché parallèle s'est développé, qui rapporte des sommes astronomiques.

L'usurpation d'identité est quotidienne dans le monde réel, mais, dans le monde virtuel, qui est aussi réel, elle correspond à une délinquance extrêmement préoccupante qu'on a encore du mal à chiffrer. Pour l'instant, l'autorité judiciaire n'appréhende qu'imparfaitement ce phénomène, même si, en termes de réponse juridique, nous disposons d'un arsenal complet.

On a tendance à considérer que l'usurpation d'identité n'est pas encore prise en compte comme un véritable délit et qu'il serait nécessaire de modifier le code pénal. En fait, il faut être beaucoup plus nuancé. Le plan numérique 2012, présenté à la fin de l'année 2008, a repris une proposition qui figurera dans la future loi d'orientation et de programmation pour la performance de la sécurité intérieure, la LOPPSI, qui sera examinée en avril, laquelle introduira dans le code pénal un article 323–8 visant à créer spécifiquement un délit d'usurpation d'identité en ligne.

De quels outils disposons-nous actuellement pour répondre au délit d'usurpation d'identité ? En fin de compte, ils sont nombreux. J'ai même découvert, en préparant cette intervention, que l'usurpation du nom d'une entreprise était réprimée. En fait, en l'état du droit pénal français, l'usurpation d'identité en elle-même est un délit pénal. Le législateur a mesuré le problème du point de vue de l'entreprise, notamment s'agissant des noms de domaine. Je ne voudrais pas vous submerger de références, mais sachez que l'article R. 20–44–46 du code des postes et des communications électroniques dispose qu'un « nom identique à un nom patronymique ne peut être choisi pour nom de domaine, sauf si le demandeur a un droit ou un intérêt légitime à faire valoir sur ce nom et agit de bonne foi ». Il est issu d'un décret de février 2007 relatif à l'attribution et à la gestion des noms de domaine de l'Internet.

Cet article commence à faire l'objet d'une application. Il revient alors à l'AFNIC, l'Association française pour le nommage Internet en coopération, de bloquer un nom de domaine lorsque celui-ci est utilisé abusivement.

En mars 2008, le juge des référés de Saint-Malo a condamné le candidat à une élection municipale qui avait enregistré des noms de domaine usurpant le nom de son concurrent.

Plus récemment, dans une ordonnance de référé du 5 janvier 2009, le tribunal de grande instance de Paris a demandé au titulaire du nom de domaine comptedeparis.fr de faire procéder à son blocage par l'AFNIC. Il a laissé trois semaines au comte de Paris pour assigner le défendeur au fond.

Ces mesures d'urgence permettent de bloquer un nom de domaine quand ce dernier est utilisé à plusieurs reprises sans que la personne puisse faire valoir un intérêt à l'utiliser de bonne foi.

Il existe un projet de réforme du code pénal et du code de procédure pénale. Ce ne serait d'ailleurs pas du luxe compte tenu de l'empilement des textes, qui rend le quotidien des spécialistes, des avocats et des magistrats assez difficile.

L'usurpation d'identité est réprimée par l'article 434–23 du code pénal, dans des cas bien spécifiques et délimités, quand celle-ci peut avoir des incidences sur une inscription au casier judiciaire. Aux termes de cet article, elle constitue un délit dès lors qu'elle intervient « dans des circonstances qui ont déterminé ou auraient pu déterminer contre [le tiers dont l'identité a été usurpée] des poursuites pénales », c'est-à-dire des incidences préjudiciables à sa personne. La peine encourue est de cinq ans d'emprisonnement et de 75 000 euros d'amende. Pour que le délit soit constitué, il est nécessaire qu'il y ait usage du nom d'un tiers. Actuellement, le problème est qu'il n'existe pas de jurisprudence tendant à assimiler l'adresse IP ou l'adresse mél au nom.

Ainsi, contrairement à ce qu'on pourrait croire, le code pénal vise spécifiquement le délit d'usurpation d'identité.

La plupart du temps, l'usurpation d'identité n'est pas une fin en soi : elle est motivée par l'appât du gain. Je pense aux fraudes, aux escroqueries. Ce sont ces agissements que le juge va sanctionner. Le délit d'escroquerie, défini à l'article 313–1 du code pénal, est puni de cinq ans d'emprisonnement et de 375 000 euros d'amende. Cet article vise explicitement l'usage d'un faux nom, c'est-à-dire l'usage du nom d'un tiers ou d'un nom imaginaire, ou d'une fausse qualité. C'est assez complexe, mais, en réalité, l'usurpation d'identité n'apparaît pas très clairement. C'est pourquoi il est prévu de créer une infraction spécifique. Je n'y suis pas opposée, à la condition de définir une politique pénale adaptée.

L'article 323–1 du code pénal, quant à lui, réprime les atteintes aux systèmes informatisés de données, c'est-à-dire « le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données ». Le législateur a prévu des sanctions extrêmement lourdes en la matière.

En réalité, ces dispositions sont très peu utilisées. Il ne suffit pas de créer de nouvelles infractions ; encore faut-il conduire une politique pénale volontariste, établir des procédures sérieuses et désigner des officiers de police judiciaire spécialisés dans les systèmes numériques. Le risque est que la procédure fasse l'objet d'une annulation et que le prévenu soit relaxé. Souvent, ce genre d'enquêtes requiert beaucoup d'énergie et une mobilisation très importante.

Je vais vous citer un exemple très intéressant. La loi du 21 juin 2004 pour la confiance dans l'économie numérique a introduit dans le code pénal un article 323–3–1 qui réprime « le fait, sans motif légitime, d'importer, de détenir, d'offrir, de céder ou de mettre à disposition un équipement, un instrument, un programme informatique ou toute donnée conçus ou spécialement adaptés » pour capter des données personnelles à des fins de revente. Ce texte a été appliqué pour la première fois en juin 2008, par le tribunal de grande instance de Saverne, qui, sur la requête de la société Microsoft, a condamné un individu qui avait développé des tutoriels de *hacking* afin de capter des données et d'usurper l'identité de personnes. Cette condamnation a suscité de nombreux articles. Néanmoins, cette disposition du code pénal reste très peu utilisée, alors qu'il est assez aisé de repérer ces kits de *phishing*, ces tutoriels de *hacking*. À ma connaissance, c'est la seule condamnation qui a été prononcée ; à tout le moins c'est la seule qui a fait l'objet d'une publication. Cela démontre bien qu'on ne peut pas répondre à des problématiques telles que l'usurpation d'identité par la seule création de nouvelles incriminations ; encore faut-il mobiliser l'ensemble des acteurs, aussi bien en amont par la prévention qu'en aval par la répression, et engager une véritable politique pénale.

Certains considèrent les conditions de poursuite et de sanction de l'usurpation d'identité comme assez incertaines. Je serai plus nuancée. Beaucoup de condamnations sont prononcées pour des faits d'escroquerie et visent aussi le *phishing*, technique par laquelle des cybercriminels se font passer pour des organismes financiers ou de grandes sociétés en envoyant des méls frauduleux, récupèrent des mots de passe de comptes bancaires ou des numéros de cartes de crédit pour détourner des fonds. Les banques et les entreprises font tout un travail de prévention pour sensibiliser les internautes.

Souvent, ce sont les conséquences de l'usurpation d'identité qui sont sanctionnées, et non l'usurpation d'identité elle-même.

L'usurpation d'identité est un moyen pour récupérer des données. Je pourrais vous citer d'autres infractions qui sont retenues pour sanctionner des cas d'usurpation d'identité. Certaines décisions ont été médiatisées. La motivation est souvent l'appât du gain, mais une autre motivation est le désir d'exister, par exemple pour un internaute, ou le désir de vengeance. En 2006, un tribunal a retenu la qualification de violence avec préméditation. C'est très intéressant, parce qu'usurper l'identité de quelqu'un revient à violer son intimité. Pour autant, ce n'est pas un crime, au sens juridique du terme, même si cela cause un préjudice extrêmement grave à la personne qui en est victime et la touche profondément.

Dans le cas présent, le coupable a été retrouvé grâce à la communication, au service d'enquête, de ses informations de connexion au site Meetic. L'homme avait créé sur ce site un profil au nom de son ancienne amie. Il s'agissait d'une vengeance à la suite d'une séparation. Les juges du tribunal correctionnel ont voulu marquer la gravité des faits, puisque l'auteur des faits, jugé en comparution immédiate, c'est-à-dire à l'issue de la garde à vue, a été condamné à une peine assez lourde d'emprisonnement avec sursis.

Plusieurs condamnations de ce type ont été prononcées. Les magistrats ont voulu dissuader les plaisantins malintentionnés d'avoir recours à cette forme de vengeance. Dans une autre affaire, la victime avait bénéficié de dix jours d'incapacité temporaire de travail. C'est dire le choc psychologique qu'elle avait subi.

Autre infraction qui peut être retenue : le faux, réprimé par l'article 441–1 du code pénal. Le *phishing*, autrement appelé le hameçonnage, et les escroqueries par téléphone mobile peuvent être appréhendées sur le plan juridique sans modification législative.

Le futur article 323–8 du code pénal est consensuel. Il fait actuellement l'objet d'une dernière concertation interministérielle et devrait être présenté en avril prochain. Il prévoit de sanctionner d'un an d'emprisonnement et de 15 000 euros d'amende le fait d'usurper, sur tout réseau informatique de communication, l'identité d'un particulier, d'une entreprise ou d'une autorité publique. Ce texte, assez complet, permettra d'appréhender la problématique des noms de domaine, que j'évoquais tout à l'heure.

Toujours est-il que, pour éviter toute redondance, il faudra harmoniser cette disposition avec d'autres dispositions du code pénal, notamment l'article que j'évoquais plus haut qui réprime déjà l'usurpation d'un nom de domaine.

J'avais prévu d'évoquer l'exemple de pays étrangers. La plupart d'entre eux appréhendent ce phénomène non pas comme une fin en soi, mais comme un moyen de commettre des fraudes, des escroqueries et d'autres infractions. Par exemple, aux États-Unis, depuis 2005, le vol d'identité constitue un délit spécifique. Les peines ont été aggravées pour les voleurs d'identité numérique qui commettent une infraction. Ainsi, on assiste à une prise de conscience au niveau international. Le *phishing* est puni aux États-Unis d'une peine de dix ans d'emprisonnement. Sauf erreur de ma part, l'État de New York vient d'adopter un texte réprimant spécifiquement l'usurpation d'identité par des moyens électroniques.

Par ailleurs, certaines condamnations ont été fortement médiatisées. Je pense à ce qui s'est passé au Maroc, où un informaticien, qui avait créé sur Facebook un profil au nom du frère du roi Mohamed VI, a été condamné à trois ans d'emprisonnement ferme en février 2008.

Parmi les États membres de l'Union européenne, seul le Royaume-Uni s'est doté d'un texte spécifique visant l'usurpation d'identité en ligne.

Même si ce n'est pas mon domaine de compétence, j'évoquerai la possibilité de mieux appréhender ce phénomène par la signature électronique ou par la biométrie. Le droit pénal a une double facette : la prévention et la répression. La prévention est fondamentale, car elle présente l'avantage de réduire le nombre de procédures qui doivent être traitées par la suite. Il faut vraiment sensibiliser l'ensemble des acteurs et des internautes, qui sont parfois un peu inconscients ou, dès lors qu'ils sont sur la toile, se sentent un peu hors-la-loi. On a parlé des réseaux sociaux : il est vrai qu'il faut vraiment sensibiliser les jeunes sur les informations qu'ils peuvent mettre en ligne et sur celles qu'il vaut mieux ne pas mettre en ligne.

Au-delà de la création d'une énième infraction, une politique pénale volontariste en la matière m'apparaît nécessaire, laquelle fait quelque peu défaut actuellement. Le garde des sceaux a pour habitude d'adresser des instructions générales sur l'ensemble des domaines qui touchent le droit pénal. Curieusement, en matière de cybercriminalité, ces instructions ne sont que très ponctuelles et balbutiantes.

J'ai la chance de coordonner un groupe de travail nouvellement créé, commun aux cours d'appel de Paris et de Versailles, qui concentrent un nombre important d'affaires. On parle même de la création d'un pôle de compétences à Paris ou commun à ces deux cours d'appel. Nous avons entrepris un travail d'harmonisation du traitement judiciaire de ces contentieux. Nous nous sommes déjà réunis trois fois. Nous collaborons avec les services d'enquête, les services spécialisés tels que l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication, l'OCLCTIC, la Direction centrale du renseignement intérieur, la DCRI, entité nouvellement créée, qui traite des affaires d'attaque de sites, y compris des sites gouvernementaux. Avec la Brigade d'enquêtes sur les fraudes aux technologies de l'information, la BEFTI, qui est un service spécialisé dépendant de la préfecture de police de Paris, nous nous efforçons de définir de bonnes pratiques pour l'ensemble de nos collègues, lesquels sont un peu désemparés.

En effet, ces contentieux suscitent des difficultés, d'une part, parce que les éléments techniques y afférents peuvent être quelque peu rebutants, d'autre part, parce qu'ils nécessitent des investigations à l'étranger. En matière de coopération internationale, les choses avancent, mais nous avons encore des progrès à faire.

L'usurpation d'identité en ligne s'inscrit dans une problématique globale du traitement judiciaire de la cybercriminalité, qui est vraiment la délinquance de demain. Elle implique de la part des acteurs, en particulier des magistrats, une forte réactivité. Or on constate souvent un décalage entre le temps judiciaire et le temps de l'Internet et des réseaux numériques. Il faut vraiment se mobiliser face à ce phénomène qui nous menace tous.

Marie Bazetoux. Merci beaucoup d'avoir dressé pour nous le panorama de ce qui se passe en France et de nous avoir donné quelques informations sur la façon dont nous pouvons nous comporter nous-mêmes.

Je vais maintenant passer la parole à Michael Lynch, qui est en quelque sorte notre vedette britannique, notre *guest speaker*. Il est responsable chez CPP au Royaume-Uni du portefeuille protection de l'identité. Il a contribué à la création de ce produit et de ce marché et participe activement au développement de la coopération entre entreprises et pouvoirs publics pour réduire les risques de fraude. Dans son intervention, il fera le point sur l'expérience du marché britannique, qui est exemplaire en Europe, tant en termes de risques que de comportement du consommateur. Michael Lynch s'exprimera en anglais et utilisera une présentation bilingue pour servir, si besoin était, de fil conducteur.

Michael Lynch.

(Cf présentation en annexe)

Guy de Felcourt. Puisque Michael s'est exprimé en anglais, je voudrais juste reprendre deux ou trois éléments qui me paraissent importants.

Premièrement, comme vous avez pu le constater grâce aux *slides* qu'il a présentés et comme nous l'enseigne notre activité au Royaume-Uni, l'usurpation d'identité a une finalité clairement financière, notamment lorsqu'elle vise à capter des numéros de carte de crédit ou les coordonnées de comptes bancaires, même si les fausses factures de téléphone ou les faux achats sur Internet sont aussi monnaie courante.

Deuxièmement, de nombreuses fraudes sont commises sur Internet, par le biais de sites plus ou moins mafieux qui s'échangent des données. C'est pourquoi nous proposons un service très utile visant à détecter la captation de données personnelles par ces sites mafieux. Nous parvenons souvent à les repérer, sans parvenir toutefois à les détruire, puisqu'ils se reconstituent à côté. J'ai été très impressionné par les résultats d'une enquête qui a pu démontrer qu'il était possible de récupérer environ 100 000 numéros de cartes bancaires françaises sur ces sites.

Troisièmement, au Royaume-Uni, le service que nous proposons avec nos partenaires a également vocation à informer et à conseiller les consommateurs pour les aider à faire face à toutes ces difficultés et à répondre aux questions qu'ils peuvent se poser à la lecture de leurs relevés bancaires, lorsqu'ils soupçonnent des transactions frauduleuses, ou pour répondre aux interrogations que suscite Internet. Ce service connaît un grand succès.

Marie Bazetoux. Comme nous avons pu le constater, le Royaume-Uni a un niveau de maturité sur ces sujets sans doute supérieur à celui de la France. Notre dernier intervenant est le chef de service de l'expertise informatique de la Commission nationale de l'informatique et des libertés, la CNIL. Il participe au comité des CNIL européennes. Ses récents travaux dans le cadre du G29 ont notamment porté sur les moteurs de recherche et les réseaux sociaux. Gwendal Le Grand décrira les différentes missions de la CNIL ainsi que les grands principes de la protection des données personnelles. Il détaillera les travaux qui sont actuellement menés, aussi bien en France qu'à l'étranger.

Je laisse donc la parole au représentant de l'institution dont les missions peuvent être résumées par la devise : « Protection, liberté, sécurité. »

Gwendal Le Grand. Je vous propose dans un premier temps de rappeler les grands principes de la protection des données et les missions de la CNIL et, dans un second temps, de prendre quelques exemples de ce que fait la CNIL en matière d'information et de sensibilisation du public et des entreprises. Je rappellerai ensuite la position de la CNIL sur les listes noires, sur ce que Michael a appelé tout à l'heure les credit bureaus, sur les systèmes de scoring ? Enfin, j'aborderai les actions de la CNIL au niveau européen, que ce soit dans le domaine des moteurs de recherche, des réseaux sociaux, ou encore de la révision du cadre législatif européen ? Sur ce dernier point, il est d'ailleurs prévu à terme d'imposer des obligations de notification des failles de sécurité. Cette mesure est actuellement en cours de discussion au niveau européen.

La CNIL, vous le savez, est l'autorité indépendante de protection des données en France. Elle encadre les traitements de données à caractère personnel. Précisément, qu'est-ce qu'une donnée personnelle ? Dans la loi « informatique et libertés » et dans la directive européenne de 1995, la notion de donnée à caractère personnel est extrêmement large, puisqu'elle toute information relative à une personne physique identifiée ou identifiable. Cela couvre toutes les données qui, directement ou indirectement, concernent une personne. Pour savoir si une donnée est personnelle, il convient de considérer l'ensemble des moyens qui sont susceptibles d'être raisonnablement mis en œuvre soit par le responsable de traitement, soit par toute autre personne. En fait, on peut croiser des données qui sont détenues par différents interlocuteurs pour déterminer si l'on a affaire ou non à une donnée à caractère personnel.

Si vous souhaitez plus de précision sur cette notion, je vous renvoie à un document qui a été publié en 2007 par le G29, qui regroupe les CNIL européennes. Il s'agit du document WP136, que vous pourrez facilement trouver via un moteur de recherche avec les mots « WP136 Avis 4/2007 ». Ce document d'une trentaine de pages contient un certain nombre d'exemples concrets qui vous expliqueront ce que recouvre la notion de donnée à caractère personnel.

Quelle est la position des CNIL européennes sur ces données à caractère personnel et comment appréhende-t-on leur protection ? Je ne vous détaillerai ni le contenu de la loi ni celui de la directive, mais je résumerai les cinq principes extrêmement généraux qui guident la réflexion en la matière.

Premièrement, le principe de finalité. Quand vous mettez en place un traitement, ce traitement doit avoir une finalité particulière bien définie.

Deuxièmement, le principe de proportionnalité. Vous devez traiter uniquement des données qui sont en rapport avec cette finalité. J'y reviendrai tout à l'heure, puisque cet élément peut être important, comme on le verra notamment par rapport aux centrales positives.

Troisièmement, la durée de conservation limitée des données. Cette durée doit être en rapport avec la finalité.

On peut résumer tout cela sous le principe de proportionnalité et de minimisation des données : vous devez traiter uniquement les données qui sont utiles à votre finalité pendant la durée qui est nécessaire à l'accomplissement de cette finalité.

Ensuite, tant la loi que la directive prévoient un certain nombre de droits pour les personnes : droits d'accès, d'opposition, de rectification des données.

Enfin, dernier principe très important, et sur lequel mon service travaille beaucoup, celui de sécurité. Quand vous traitez des données à caractère personnel, vous êtes tenus de les traiter dans un environnement qui est suffisamment sécurisé. Cela renvoie aux exemples cités tout à l'heure de pertes de données à caractère personnel. Ces pertes s'expliquent soit par une collecte trop importante, soit parce que le traitement lui-même n'était pas suffisamment sécurisé. Par exemple, le disque dur du PC portable sur lequel se trouvent les données n'est pas chiffré ; ou bien les serveurs FTP qui contiennent ces fichiers, ces données, y compris des données bancaires, ne sont pas suffisamment protégés des indexations permises par les moteurs de recherche. C'est pourquoi la CNIL est amenée à faire des recommandations aux sociétés qui détiennent des données à caractère personnel pour que le traitement de celles-ci soit suffisamment sécurisé. Elle est également amenée à vérifier les mesures de sécurité mises en place dans les entreprises dans le cadre de ses missions de contrôle.

Quelles sont les grandes missions de la CNIL ?

Premièrement, elle a une mission d'information et de conseil, tant en direction des autorités que des professionnels et du grand public.

Deuxièmement, elle a un rôle de régulateur et de contrôle des fichiers, son rôle le plus connu. Elle exerce deux types de contrôle : le premier, très connu, est le contrôle a priori. Quand vous mettez en place un fichier contenant des données à caractère personnel, vous devez en général le déclarer à la CNIL. En fait, il existe différent types de formalités : soit une simple déclaration suffit, soit certains traitements sont soumis à une autorisation de la CNIL.

Dans ce cas, cela signifie que celle-ci peut autoriser le traitement ou bien refuser qu'il soit mis en oeuvre. Les traitements susceptibles d'exclure des personnes du bénéfice d'un droit, d'une prestation ou d'un contrat en l'absence de disposition législative ou réglementaire (comme les listes noires, notamment), sont soumis à autorisation de la CNIL.

La CNIL exerce également un contrôle a posteriori. Celui-ci date de la loi de 2004. Concrètement, la CNIL dispose d'un service qui peut effectuer des contrôles sur place, vérifier auprès d'un responsable de société à quel type de traitement de données à caractère personnel il procède, et s'assurer que ce traitement est bien conforme à la loi « informatique et libertés ».

Évidemment, si des manquements sont constatés, la loi prévoit que des sanctions peuvent être prononcées par la CNIL, puisqu'un pouvoir de contrôle n'a véritablement de sens que s'il est assorti d'un pouvoir de sanctions.

Deux autres points sont également intéressants.

D'une part, depuis 2004, les sociétés peuvent disposer d'un correspondant « informatique et libertés », un CIL. Celui-ci est informé des traitements de données à caractère personnel. La présence d'un tel correspondant exonère d'un certain nombre de formalités, notamment les déclarations auprès de la CNIL. Aujourd'hui, environ 1 000 correspondants ont été déclarés à la CNIL, sachant qu'un CIL peut agir pour plusieurs sociétés. En 2008, 3 700 sociétés étaient dotées d'un correspondant.

Autre pouvoir qui pourra être intéressant à terme pour l'information des personnes et la promotion de meilleurs outils de sécurité : le pouvoir de labellisation. A l'avenir, la CNIL aura la possibilité de dire qu'un produit respecte ou non les principes de la loi « informatique et libertés ». C'est intéressant à la fois pour la personne qui développe le produit, qui pourra ainsi promouvoir son produit et éventuellement se démarquer de la concurrence, mais aussi pour le consommateur, qui utilisera ce produit tout en étant assuré que celui-ci atteint un certain niveau de qualité. Ce sera également intéressant lors de la rédaction d'un cahier des charges.

La CNIL compte environ 120 agents. Nos ressources sont inférieures à ce dont disposent nos homologues européens. Par exemple, la CNIL allemande compte environ 400 agents, pour une population à peu près équivalente. Nous recevons environ 70 000 déclarations par an. Les plaintes dont la CNIL est saisie peuvent donner lieu à des contrôles sur place. En moyenne, nous recevons entre 4 000 et 4 500 plaintes par an. C'est significatif.

J'en viens maintenant aux actions plus spécifiques.

Premièrement, les actions de la CNIL à destination du public, des entreprises, des parlementaires, etc.

Le site Internet de la CNIL contient des rubriques à destination des jeunes et du grand public pour les sensibiliser aux dangers d'Internet. On trouve également des dossiers plus détaillés pour expliquer certaines technologies, ainsi que des guides très utiles.

Récemment, la CNIL a édité un guide à destination des employeurs pour leur expliquer ce qu'il est possible de faire en matière notamment de vidéosurveillance sur le lieu de travail, de cybersurveillance des employés, de mise en place de la biométrie, etc.

La CNIL dispense également, via les médias, de l'information à destination du grand public. Ainsi, depuis un peu plus d'un an, nous disposons d'une rubrique hebdomadaire sur France Info, tous les mercredis à 11 h 45. Cette rubrique présente des cas concrets où le citoyen est confronté à des problématiques de vol d'identité, de spams, de gestion de données à caractère personnel, etc.

La CNIL a également mis en place une information à destination de différentes catégories de la population. L'année dernière, nous avions identifié deux catégories qui étaient particulièrement mal informées en matière de protection des données : les jeunes et les parlementaires.

S'agissant de la première, une convention de partenariat a récemment été signée avec la défenseure des enfants pour mettre en place une campagne d'information nationale qui inclut non seulement les jeunes, mais encore toutes les personnes qui travaillent à leur contact, à savoir les éducateurs, les enseignants, etc.

De manière plus inattendue, les parlementaires sont assez peu sensibilisés en matière de protection des données. Aussi, le président de la CNIL a obtenu d'être régulièrement auditionné par les commissions de l'Assemblée nationale et du Sénat et par l'Office parlementaire d'évaluation des choix scientifiques et technologiques.

L'information se fait aussi en direction des entreprises. La CNIL est souvent amenée à faire un certain nombre de recommandations en matière de sécurité quand un dossier lui est soumis. Dans certains cas, la CNIL a pu définir un cadre particulier dans une recommandation (comme pour le vote électronique) ou dans le cadre de formalités simplifiées – il s'agit alors de formalités du type « normes simplifiées » ou « autorisations uniques » –, dans d'autres cas, les recommandations sont formulées au cas par cas dans le cadre de l'instruction des dossiers. Quelles qu'elles soient, elles sont toujours le fruit d'un dialogue avec les entreprises.

Par exemple, nous avons parlé tout à l'heure des réseaux sociaux. Nous sommes en contact avec ceux-ci depuis longtemps afin qu'ils mettent en place notamment des outils permettant de gérer le niveau de diffusion des données à caractère personnel.

Nous sommes aussi en relation avec toutes les entreprises qui mettent en place des démarches en collaboration avec la CNIL, pour leur faire des recommandations en vue d'une meilleure sécurité de leur traitement des données à caractère personnel.

Par ailleurs, on voit bien, à travers les exemples qui ont été cités en introduction, que ces phénomènes de pertes de données à caractère personnel s'amplifient aujourd'hui, d'autant plus que les technologies de l'information sont de plus en plus présentes dans notre environnement et qu'il existe de plus en plus de services mobiles. Les PC portables ou les téléphones mobiles ne sont pas forcément chiffrés, pas plus que ne le sont les données qui y sont conservées – voyez ce qui s'est passé au Royaume-Uni avec des données fiscales non chiffrées qui était conservées sur des CD-ROM. Aussi, nous sommes amenés à recommander l'utilisation d'outils simples, si possible des outils qui ont fait l'objet d'une évaluation et qui présentent des garanties en matière de sécurité, permettant de chiffrer le disque dur par exemple.

Si vous mettez votre PC au rebut sans avoir correctement effacé les données qu'il contient, celles-ci peuvent parfaitement être récupérées. Je vous renvoie aux exemples concrets qui ont été cités tout à l'heure. La Direction centrale de la sécurité des systèmes d'information, la DCSSI, a recensé, évalué et certifié un certain nombre de produits qui présentent toutes les garanties en matière de sécurité et qui vous permettront de chiffrer ou d'effacer en toute quiétude les données de votre disque dur. Cette liste est disponible sur le site de la DCSSI.

Quand vous placez un fichier dans la corbeille, vous pensez qu'il a été détruit. En réalité, vous avez simplement libéré de votre disque dur l'espace sur lequel il était enregistré. De fait, il y est toujours présent et peut être retrouvé. En revanche, si l'on réécrit sur cet espace, alors les anciennes données sont réellement effacées.

Le traitement des données à caractère personnel dans les grandes sociétés multinationales peut également soulever quelques problèmes. En effet, pour développer des applications, il faut généralement travailler sur des données tests. Or, trop souvent, le développement de ces applications se fait à partir de données réelles. Pour aggraver le problème, ce développement est la plupart du temps externalisé à l'étranger, par exemple en Inde.

Je précise que je n'ai rien contre ce pays, mais celui-ci ne fait pas partie des pays dont on considère qu'ils offrent un niveau de protection des données adéquat. Pour autant, ils sont experts dans le développement des applications.

Il existe donc un certain nombre de pays vers lesquels est externalisé le développement des applications sans qu'il soit possible de contrôler la manière dont ceux-ci traiteront les bases de données sur les clients.

De la même manière, une entreprise est parfois amenée à envoyer un disque dur qui a planté, à une société de maintenance sans s'être assuré préalablement que les données qu'il contenait avaient bien été effacées, alors même que ces données devraient être protégées et devraient rester dans le périmètre physique de l'entreprise.

Aussi, nous sommes amenés à discuter avec les responsables informatiques pour nous assurer que des mesures de protection des données, y compris lors de ces opérations, sont bien mises en place.

J'en viens au deuxième thème qui vous intéresse en tant que société d'assurance ou organisme de crédit : la problématique des listes noires, des centrales positives et des systèmes de scoring.

Les listes noires ont pour vocation d'exclure une personne du bénéfice d'un droit, par exemple l'accès à un logement ou à un crédit. Il faut savoir que, conformément à l'article 25 de la loi, tous les traitements d'exclusion sont soumis à une autorisation de la CNIL. C'est pourquoi la Commission s'est intéressée à ces questions depuis longtemps.

Un rapport d'ensemble sur les listes noires a été publié en 2003, dont je vous rappellerai brièvement les orientations.

Premièrement, les listes noires ne peuvent pas être secrètes. Vous devez informer les utilisateurs que vous mettez en place des listes noires ; vous devez également les informer des critères justifiant leur inscription sur une liste noire. Cette information doit être dispensée à trois moments : lors de la collecte des renseignements ; lors de la survenance de l'incident qui peut donner lieu à un fichage ; le cas échéant, lors du fichage.

Deuxièmement – cela rejoint le principe de finalité –, pas de mise au pilori. Concrètement, si j'ai été exclu du bénéfice d'un crédit, pour autant, je ne dois pas être exclu du bénéfice d'un logement. L'utilisation de ce système est limitée à un secteur particulier et les informations doivent être traitées avec une finalité bien précise.

Troisièmement, garantir le droit à l'oubli. Cela rejoint le principe de durée de conservation des données, que j'ai évoqué précédemment.

Quatrièmement, assurer la sécurité et la confidentialité des données. C'est encore l'un des grands principes de protection des données que je citais tout à l'heure. Le responsable du traitement est obligé de mettre en place des mesures de sécurité concrètes techniques et organisationnelles de manière que le système soit suffisamment sécurisé et garantisse une correcte protection des données à caractère personnel.

D'autres systèmes ont été évoqués tout à l'heure par Michael Lynch, à savoir les centrales positives, ce qu'on appelle les credit bureaus au Royaume-Uni et aux États-Unis. Ces centrales positives recensent, sur les personnes, des informations non seulement négatives – si ce sont des mauvais payeurs, par exemple –, mais également positives – sur leur patrimoine, sur leurs crédits. Ces systèmes se sont beaucoup développés aux États-Unis et au Royaume-Uni. Dans ces deux pays, les informations détenues par ces centrales sont accessibles à des personnes situées hors de la sphère financière, par exemple les bailleurs ou toute personne justifiant d'un rôle professionnel particulier.

Ce système s'est répandu également dans un certain nombre de pays européens comme l'Allemagne, la Belgique, l'Autriche. Mais dans ces pays, l'accessibilité aux informations est restreinte aux personnes évoluant dans la sphère financière. Le périmètre des centrales positives n'y est pas aussi large qu'au Royaume-Uni et qu'aux États-Unis.

Avec ces centrales positives, le risque est que beaucoup d'acteurs aient accès aux informations qu'elles détiennent, y compris ceux qui sont situés hors de la sphère financière. Je fais ici le lien avec le principe de finalité que j'évoquais tout à l'heure.

L'autre problème, c'est un risque par rapport aux personnes. Aux États-Unis, 90 % de la population sont fichés par ces centrales positives et l'absence de référencement dans leurs fichiers constitue un facteur d'exclusion. Cela soulève évidemment un problème.

Enfin, des erreurs peuvent survenir dans la tenue de ces fichiers, soit parce que, leur périmètre étant très large, les informations qu'ils contiennent ne sont pas à jour, soit en raison d'homonymies.

Ces systèmes ont une double finalité : prévenir le surendettement et favoriser le crédit à la consommation en permettant à des personnes qui en auraient été exclues par les méthodes traditionnelles de scoring, d'y accéder.

La CNIL a une position relativement réservée sur les centrales de crédit. En 2007, ayant reçu une demande d'autorisation, elle a prononcé un refus en se fondant sur trois critères : premièrement, il y avait une transmission massive d'informations personnelles à une société qui n'était pas couverte par le secret bancaire ; deuxièmement, les personnes concernées devaient signer une clause de levée du secret bancaire sans qu'elles soient correctement informées ; enfin, la quantité d'informations traitées excédait largement ce qui était raisonnablement requis pour décider ou non l'attribution d'un crédit.

Guy de Felcourt. Il paraît que l'Assemblée nationale se saisira de cette question à la fin du mois.

Gwendal Le Grand. Justement, c'est le dernier point que je voulais mentionner au sujet de ces centrales positives et notamment au sujet de l'examen de la demande d'autorisation dont je vous parlais.

La CNIL a estimé qu'il ne lui appartenait pas de se prononcer pour ou contre la mise en place de ces systèmes. Au contraire, elle pense qu'il appartient au Parlement de déterminer la pertinence et les règles de fonctionnement de ces centrales positives. Un examen de cette question par le parlement irait complètement dans le sens des préconisations qu'avait faites la CNIL lors de son refus d'autorisation en 2007.

Enfin, troisième méthode, très répandue, celle du scoring, qui consiste à évaluer le risque de défaillance d'un emprunteur en fonction de critères statistiques fondés sur le comportement des précédents emprunteurs. Les systèmes de scoring sont soumis à un régime simplifié d'autorisation préalable de la CNIL sous forme d'autorisation unique modifiée en 2008 –. Je vous renvoie à notre site Internet pour de plus amples informations sur ce régime.

L'un des points essentiels pour la CNIL est que ces systèmes de scoring doivent être des outils non pas de prise de décision, mais d'aide à la décision, laquelle ne doit pas se fonder uniquement sur les données fournies par le système de scoring. Le régime de l'autorisation unique impose que, en cas de refus d'un crédit sur le seul fondement du système de scoring, le client voie sa demande réexaminée manuellement.

Pour terminer, je voudrais mentionner certains travaux que mène la CNIL au sein du comité des CNIL européennes, le G29.

Nous avons évoqué tout à l'heure les travaux sur les moteurs de recherche. Effectivement, en 2008, le G29 a publié un avis sur les moteurs de recherche. Je m'attarderai seulement sur trois de ses conclusions.

Premièrement, même quand le traitement est effectué par une société comme Google, qui est principalement basée aux États-Unis, la législation européenne en matière de protection des données s'applique et les critères définis par la loi « informatique et libertés » doivent être respectés.

Deuxièmement, une directive européenne sur la conservation des données de connexion a été transposée en droit français. Elle oblige les opérateurs de communications, par exemple les fournisseurs d'accès à Internet ou les opérateurs en téléphonie mobile, à conserver en France les données de connexion pendant un an. Dans l'avis du G29, il est indiqué que cette directive ne s'applique pas aux moteurs de recherche, car ce sont des services de la société de l'information qui sont explicitement exclus du périmètre de la directive sur la conservation des données. Autrement dit, les moteurs de recherche ne sont soumis à aucune obligation légale de conservation des données de connexion.

Troisièmement, nous avons examiné les raisons pour lesquelles sont collectées des données à caractère personnel dans les moteurs de recherche, notamment à travers des questionnaires. Nous sommes parvenus à la conclusion que, à l'heure actuelle, il n'existait aucune raison objective pour que ces données soient conservées plus de six mois. Simplement, qu'entend-on par « durée de conservation par les moteurs de recherche » ? Chaque fois que vous faites une requête au moyen d'un moteur de recherche, celui-ci conserve l'adresse IP de votre machine, autrement dit l'identité de cette machine et dépose un identifiant unique appelé cookie, qui est déposé par le moteur. Ces données sont notamment associées aux requêtes adressées par un utilisateur ; c'est-à-dire que les moteurs de recherche sont capables de lister l'ensemble des requêtes d'un utilisateur pour une durée qui varie en fonction du moteur utilisé.

Depuis que les CNIL européennes ont recommandé des durées de conservation n'excédant pas six mois, celles-ci ont fortement diminué, puisque Google a par exemple annoncé les avoir réduites de moitié.

Dans un autre domaine, toujours au niveau européen, la CNIL a été très active dans la révision du « paquet télécom ». Le paquet télécom est un ensemble de directives concernant le cadre réglementaire des réseaux et services de communications électroniques dans l'Union européenne et incluant notamment la directive « vie privée et communications électroniques ». Il est prévu d'introduire dans cette dernière une obligation de notification des failles de sécurité qui s'appliquerait aux opérateurs de communications électroniques et peut-être aux services de la société d'information. Aujourd'hui, ce n'est pas complètement arrêté. Le Parlement et les autorités de protection des données souhaitent que l'obligation de notification soit la plus large possible, alors que la Commission européenne et le Conseil ne semblent pas favorables à une obligation de notification qui couvrirait les services de la société de l'information. Il faut savoir qu'aux États-Unis cette obligation de notification est très large. Au Royaume-Uni, cela a été évoqué tout à l'heure, il existe un système de notification volontaire à l'Information commissioner's office, qui est l'équivalent de la CNIL.. Rendre publiques ces failles de sécurité contribuerait à une meilleure information des personnes. La CNIL souhaite que cette obligation soit applicable non seulement aux opérateurs de communications, mais également aux services sur Internet. Si tel était le cas, l'information des personnes et les pratiques des responsables de traitement en matière de sécurité s'en trouveraient indéniablement améliorées.

Ce débat n'est pas complètement clos. Le Parlement votera en mai 2009, et la directive révisée devrait être a priori adoptée dans le courant de l'année. On connaîtra à ce moment-là le périmètre de l'obligation de notification des failles de sécurité. En tout cas, le principe est accepté au moins pour les opérateurs de communications à l'intérieur du paquet révisé.

En conclusion, vous l'avez compris, le périmètre d'action de la CNIL est extrêmement large. Elle joue un rôle très important dans la protection des données, à travers son rôle de régulation et d'information. Il ne faut pas la considérer comme un empêcheur d'innover, un censeur. Elle est là aussi pour vous accompagner et vous conseiller en amont, pour aider les entreprises à innover d'une manière responsable en mettant en œuvre de meilleures pratiques en matière de protection des données et de sécurité des traitements et afin que la loi soit respectée.

Marie Bazetoux. Bravo et merci beaucoup. Je vais maintenant demander à mon voisin, Stéphane Koch, qui s'est livré, pendant que nous parlions, à quelques exercices avec son téléphone, de nous dire si, quand il a allumé celui-ci, il a détecté d'autres appareils.

Stéphane Koch. Oui, un certain nombre d'appareils étaient allumés dans un périmètre très restreint, détectés par Bluetooth, dont mon téléphone est équipé. Cette technologie est efficace jusqu'à 10 mètres.

Si j'avais de mauvaises intentions, et si mon téléphone disposait des programmes adéquats, je pourrais accéder aux carnets d'adresses ou aux données contenues dans les téléphones environnants. Il faut être conscient des risques que fait courir Bluetooth et être très prudent !

Encore plus problématiques sont les *laptops*. Tous sont équipés de Bluetooth, et les gens ne sont pas forcément conscients que cette technologie est une porte d'entrée parallèle sur leur *laptop*. Même chez vous, si votre voisin utilise Bluetooth avec son *laptop* pour détecter les ordinateurs environnants, s'il détecte votre ordinateur, il lui sera alors loisible de pénétrer dans votre machine, quand bien même celle-ci serait protégée par un *firewall* qui, aussi performant soit-il, serait incapable de gérer Bluetooth.

Il faut bien avoir conscience que ces technologies sont d'autant plus omniprésentes qu'elles sont vendues sous forme de *package*. Aujourd'hui, les appareils disponibles dans le commerce, surtout ceux que l'on appelle les appareils intelligents, par exemple les *smartphones*, intègrent des systèmes d'exploitation qui en font de véritables ordinateurs portables. A une époque, on vendait des routeurs *Wifi* sans informer l'acheteur des mesures de protection qu'il devait prendre.

Marie Bazetoux. Bien noté !

Voici venu le temps du débat. Nous vous laissons la parole. A vous.

Débat

Question. Chez moi, j'utilise un logiciel afin d'effacer, d'une part, les données contenues sur mon disque dur, d'autre part, mes traces de connexion lorsque j'interroge mon compte bancaire. Ces logiciels sont-ils efficaces ? Comment peut-on faire pour se protéger lorsqu'on utilise, dans un lieu public, un portable équipé de Bluetooth ? Comment puis-je protéger mon Blackberry ? De quels moyens de protection dispose-t-on pour se protéger contre ces risques d'intrusion ?

Stéphane Koch. Un certain nombre d'éléments ont été abordés au cours des différentes présentations.

Premièrement, il faut chiffrer vos données, limiter le risque à une perte matérielle et éviter toute perte d'informations. Deuxièmement, considérer chaque ordinateur portable comme une valise. Si l'on quitte son entreprise avec son ordinateur portable, il ne faut y introduire que les données dont on a besoin, à l'exclusion de toute autre, par exemple des informations sur son entreprise, même si les disques durs sont maintenant dotés d'une très grande capacité. Quant à *Bluetooth*, libre à vous de l'activer ou non, de le rendre détectable ou indétectable en fonction de vos besoins et de vos usages.

S'agissant des programmes, je conseille plutôt ceux que l'on appelle *open source*, qui, parce qu'ils sont développés en communauté, sont soumis à une sorte d'autocontrôle de manière qu'ils ne contiennent pas de programmes malicieux. Aujourd'hui, certains antivirus gratuits contiennent en fait des chevaux de Troie pour accéder à votre machine. Un programme en *open source* vous permettra d'exercer cet autocontrôle. Par exemple, le programme *Eraser* vous permet de supprimer efficacement les données de votre disque dur, sans avoir à débourser quoi que ce soit.

Quant aux traces, il s'agit d'un autre problème. Quand je vous parlais des 52 000 comptes UBS sur lesquels le fisc américain a demandé des informations, on peut s'interroger sur la traçabilité. Le *Patriot act* autorise les services américains à accéder à tout moment et sans justification à ces informations. Or, même si vous effacez les traces de votre machine, celles-ci seront conservées par votre fournisseur d'accès, qui dispose d'outils de profilage très évolués.

Maintenant, si vous passez par ce qu'on appelle un *proxy*, c'est-à-dire un ordinateur tiers, pour vous connecter à tel ou tel site, peut-être serez-vous plus difficilement identifiable, mais il faudra déjà connaître le *proxy* auquel vous avez eu recours pour être certain qu'il est sûr. De surcroît, votre navigation s'en trouvera ralentie.

Il n'existe pas de solution unique. Il faut trouver un équilibre. Ce n'est pas parce qu'on protège une information sur un disque dur que celle-ci est inviolable. Si votre mot de passe est très simple, il est possible de le cracker et d'accéder à l'information chiffrée. C'est un vrai problème sur les réseaux sociaux. Beaucoup de gens utilisant des mots de passe simples, il est possible d'accéder à leur compte en connaissant uniquement leur adresse mél et leur nom. Il existe une multitude de services fonctionnant avec des bases de données. Ces services, d'un accès libre, ne trouvent pas leur équilibre financier. A tout moment, ils peuvent être vendus, faire faillite. Qu'adviendra-t-il des données en leur possession ? Pourront-elles être vendues à des tiers, par exemple à des sociétés de marketing, voire être bradées ? Comme on l'a vu avec Facebook, les conditions générales d'utilisation peuvent subitement évoluer à votre corps défendant.

Guy de Felcourt. Il existe de multiples façons de perdre des données : une fuite dans une entreprise, des identifiants subtilisés sur Facebook ou un paiement par téléphone qui a été intercepté. Le Centre de recherche pour l'étude et l'observation des conditions de vie, le Credoc, a récemment conduit une étude qui a montré qu'une poubelle sur quatre contenait des données personnelles importantes. Les causes et les formes d'usurpation d'identité sont par conséquent très diverses.

On estime actuellement que 1 % du trafic Internet est détourné en raison des failles structurelles qui affectent les messageries. On dispose maintenant d'outils informatiques pour détecter les failles sur les sites *web*, de services d'assistance, de conseils d'experts qui peuvent, si nécessaire, procéder à des investigations. Il faut éduquer le consommateur, l'inciter à la prudence, par exemple en lui conseillant de ne pas communiquer sa date de naissance sur Facebook.

Beaucoup de banques et d'établissements financiers distribuent à leurs clients des certificats d'authentification, qui peuvent être des mots de passe dynamiques, du *3D Secure*, ou des mini-terminaux avec signature électronique. Il y a ainsi une dualité : d'un côté, on fait tout pour sécuriser notre navigation ; d'un autre côté, on nous explique que le monde numérique n'est pas sûr et l'on nous propose des services destinés à nous rassurer, à nous informer, à résoudre nos problèmes.

Gwendal Le Grand. Évidemment, il existe des solutions pour effacer ou chiffrer un disque dur. Je vous renvoie au site de la DCSSI, qui référence un certain nombre de produits qui, évalués et certifiés, garantissent un certain niveau de qualité. Mais une fois que vous avez partagé vos données sur Internet, c'est terminé ! Vous ne les maîtrisez plus, vous dépendez de la manière dont le responsable du site va les traiter. Si vous communiquez votre numéro de carte bleue à un hôtel et que celui-ci le stocke sans précaution, rien n'empêche que ce numéro soit divulgué. Il est très difficile d'effacer ces données, car vous ne savez pas où elles sont, vous ne savez pas combien de fois elles ont été reproduites. Tant que vous avez encore les données sur votre disque dur, vous êtes à même de les détruire correctement puisque vous êtes la seule personne à les posséder. Sur Internet, vous dépendez des mesures qui sont mises en place par des tiers et des pratiques de ces derniers.

Stéphane Koch. Derrière chaque infrastructure de sécurité, il y a des hommes. Et l'homme est faillible. Ma connexion Orange est sécurisée, chiffrée, et interdit tout accès intempestif à mes données. Mais vous n'avez aucune garantie qu'un des salariés d'Orange, lesquels ont accès à cette information, ne va pas, pour une raison quelconque, trahir son employeur. Personnellement, j'ai travaillé pour une société de télécommunications suisse. Une fois, un détective privé m'avait proposé quelques milliers d'euros en échange des plans d'une villa qui lui auraient permis de placer des écoutes. Ainsi, le risque humain est encore plus difficilement gérable que le risque technologique. Il existe une zone tampon sur laquelle il est impossible d'intervenir et qui nécessite une protection différente.

Gwendal Le Grand. En effet, lors de la constitution de fichiers, nous demandons toujours, parmi les mesures de sécurité, un contrôle du contrôle. Il est toujours possible, grâce à des systèmes de traçabilité, de savoir qui a accédé à quelles données. Nous vérifions que cette traçabilité est correctement assurée et que les fichiers de trace sont également surveillés. Chez Orange, par exemple, certains salariés sont habilités à accéder à un certain nombre d'informations personnelles ; cela fait partie de leur travail. En contrepartie, on doit savoir, grâce à ces systèmes de traçage, à quels fichiers ces personnes ont eu accès, ce en quoi a consisté leur intervention, pour être capable d'exercer un contrôle a posteriori et déterminer s'il y a eu des abus. Encore une fois, cela fait partie des points dont nous nous assurons à la CNIL. Cela vaut aussi bien pour les fichiers de police ou les traitements mis en œuvre par l'Etat que pour les fichiers gérés par les entreprises privées.

Question. Madame Quéméner, j'ai le sentiment que les FAI et les opérateurs mobiles pourraient coopérer bien davantage pour lutter contre la fraude. Tout le monde reçoit des spams ou des SMS non désirés. Aucun des trois opérateurs ne semble vraiment agir efficacement contre ces SMS.

Par ailleurs, tout le monde parle de fraude ou d'usurpation d'identité, mais il ne faut pas oublier que, grâce à Internet, on peut souvent retrouver un vieux camarade de classe ou rendre publique son expertise dans le monde entier. Généralement, j'ai plutôt tendance à rappeler les dangers d'Internet, mais, pour autant, il ne faudrait pas négliger la globalisation de l'information qu'il permet.

Myriam Quéméner. Sans doute ne serai-je pas la seule personne compétente pour commenter votre propos.

Effectivement, les FAI ont la possibilité de signaler les spams. C'est d'ailleurs ce à quoi s'emploie Signal spam, exemple de coopération publique-privée. Il n'en demeure pas moins que des progrès doivent être réalisés en la matière. La cybercriminalité implique de nouveaux comportements de la part des différents acteurs. Je m'entretenais récemment de ce sujet avec un juriste de Microsoft, qui parlait de « choc des cultures ».

La situation évolue, et le Conseil de l'Europe a pris des initiatives en la matière. Il faut que les services d'enquête spécialisés et les offices collaborent avec les FAI. La justice reste un peu timorée et hésite encore à associer les FAI à ces réflexions. Je suis d'accord avec vous : nous sommes inondés de spams, y compris dans des lieux qui devraient être sécurisés, comme les sites ministériels ou les sites de juridictions. A la cour d'appel, nous sommes inondés de spams. Ce phénomène a d'ailleurs tendance à s'accentuer, y compris pour les particuliers, notamment en période de crise. Sans doute connaissez-vous le rapport rédigé par la LCEN (Loi pour la Confiance de l'Economie Numérique) dans lequel les FAI sont montrés du doigt. Ceux-ci doivent faire des progrès pour respecter les obligations auxquelles ils sont soumis. Je pense notamment à la lutte qu'ils doivent mener contre les atteintes à la dignité humaine. Ils doivent faire connaître aux autorités publiques les moyens d'action qu'ils ont mis en œuvre.

Christine Naudin. Je souscris à vos propos. Oui, Internet est un outil formidable. De façon générale, il vaut mieux positiver plutôt que de sombrer dans la paranoïa.

Je reviens à la question du premier intervenant, qui demandait comment l'on pouvait effacer de manière sûre des données contenues sur un disque dur. Par ma maigre expérience, je sais que les délinquants un peu chevronnés utilisent *Evidence Eliminator*.

Je vous ai parlé d'une société basée sur la confiance. C'était vrai voilà 30 ou 40 ans. Aujourd'hui, c'est fini. On découvre que, dans un monde global, on ne peut plus se baser uniquement sur la confiance et considérer que 99 % des gens seraient honnêtes. Ce n'est pas le cas. Nous sommes obligés de prendre des mesures, ce que MM. Le Grand et Koch ont très bien expliqué. Mais il ne faut pas non plus vivre dans une totale paranoïa. Au-delà du contrôle et du contrôle du contrôle, si l'on veut maintenir et préserver les libertés individuelles et, surtout, les libertés collectives que l'on a acquises à prix fort au cours de l'histoire, il faut se garder du principe de précaution permanent : manger un yaourt dont la date limite de consommation est à peine dépassée, c'est dangereux ; avoir son téléphone portable collé à l'oreille, c'est dangereux ; passer à côté d'une enseigne lumineuse qui émet des rayonnements électromagnétiques, c'est dangereux. On ne peut pas vivre ainsi ; la société n'évoluerait pas. Il faut dédramatiser. On a déclaré des choses fortes aujourd'hui.

Certes, les problèmes que nous avons évoqués sont réels. En tant que criminologue, je suis le premier à m'intéresser à ces problématiques. Pour autant, restons lucides. Le monde ne marche pas si mal ; contrairement à ce qu'on dit, tous les politiques ne sont pas des pourris. On essaie de faire avancer la société, vous y participez et nous y participons, de façon qu'on aille vers un monde meilleur.

Je suis d'accord avec monsieur : Internet est un outil formidable. Pour cette raison, il faut qu'on puisse continuer de communiquer, qu'on puisse dire, si on le souhaite et sans que cela nuise : « Voilà ! J'existe ! J'ai travaillé dans le passé chez Gras Savoye où j'occupais tel poste ». Mais il faut prendre des mesures pour se protéger.

Stéphane Koch. Personne ne remet en cause Internet, qui, effectivement, est un outil formidable. Je ne demande pas aux gens d'être paranoïaques ; je leur demande simplement de maîtriser les outils qu'ils utilisent. Facebook est aussi un outil formidable. Parmi mes élèves, 140 disposent d'un profil sur ce site. Quant à moi, j'ai configuré mon compte de telle sorte que certaines informations n'apparaissent pas, par exemple mes relations. Je fais aussi de la sensibilisation. L'autre jour, l'une de mes élèves laisse un message déclarant qu'elle utilise Torrent pour télécharger les séries – Torrent est un outil pour faire du téléchargement pirate ! J'ai ajouté à la suite de son message : merci beaucoup ! Ici, c'est le GISTEP, entreprise spécialisée dans la détection des fraudeurs, nous vous remercions pour votre collaboration, et nous espérons que d'autres personnes suivront votre exemple et se dévoileront publiquement de cette manière !

Il existe des solutions, mais il faut faire attention à la manière dont on décrit les choses. Je suis contre le tout-juridique. Je m'oppose totalement à ce que Microsoft puisse engager des actions judiciaires contre de petits *hackers*. J'établis une distinction entre le *hacking* éthique et les cybermercenaires, la cybercriminalité professionnelle. Le *hacking* éthique est utile à notre société.

Voilà deux ans, la puce des passeports biométriques Mifare a été crackée lors de la réunion annuelle du *Chaos communication congress*, à Berlin. De même, un *hacker* britannique a démontré qu'on pouvait introduire une nouvelle fois des informations dans cette puce.

Si cette information n'est pas divulguée et qu'un problème survient avec votre passeport, comment pourrez-vous vous défendre ?

Il en va de même avec les cartes de crédit. On prétend qu'elles sont inviolables et que seuls ceux qui en connaissent le code secret peuvent les utiliser. Eh bien non ! On a prouvé au cours de l'un de ces congrès de *hackers* que cette protection pouvait être contournée. Il est important que les utilisateurs de ces cartes en soient informés.

Tout n'est pas blanc, tout n'est pas noir ; il existe une voie médiane. Condamnons les cybercriminels, mais utilisons ces *hackers*, qui mettent au jour et exploitent des failles dont sont responsables les fabricants de logiciels. Ces derniers ont donc une lourde responsabilité. Si leurs produits pouvaient être testés par la communauté avant qu'ils ne les mettent sur le marché, peut-être les risques liés à la sécurité seraient-ils bien moindres.

Question. Je ne suis pas forcément du même avis que vous concernant l'insécurité numérique. Je pense qu'elle annonce plutôt la fin d'Internet tel qu'on le connaît aujourd'hui. Par ailleurs, je voudrais savoir si vous tous travaillez avec les *hackers*. Enfin, je voudrais connaître les actions de la CNIL contre la cybercriminalité.

Stéphane Koch. Certains projettent de développer un nouvel Internet, estimant impossible de sécuriser Internet tel que nous le connaissons actuellement. N'oublions pas qu'Internet n'a pas été développé pour être sécurisé. Au départ, il s'agissait d'un projet militaire qui devait permettre de communiquer dans n'importe quelle circonstance. Depuis lors, certains protocoles ont évolué. N'oublions pas la responsabilité des tiers. S'il existe des failles de sécurité dans le système d'un nom de domaine, il est possible d'intervenir en sécurisant le système qu'on gère. Si les États ou les gestionnaires de noms de domaine ne prennent pas le soin d'implémenter des systèmes de sécurité, cela relève de leur responsabilité. Mais le problème n'est plus celui de la sécurisation possible ou impossible. Il appartient aux détenteurs d'informations et aux fabricants de logiciels eux-mêmes de s'y employer.

Le projet de nouvel Internet me semble quelque peu utopique. Comment imaginer remplacer l'existant ? Il me paraît très difficile de définir l'avenir de Internet, qui est un environnement chaotique, au sens positif du terme. Les organisations s'y font de manière spontanée. Parfois, le développement et la recherche conduisent tout à coup à reconsidérer l'existant. C'est peut-être ce à quoi nous amèneront les développements futurs et peut-être l'environnement dans lequel nous évoluons pourra-t-il être réellement sécurisé.

Pour répondre à la seconde question, je vous confirme que je fréquente un certain nombre de *hackers*. Il est délicat de parler de travail à leur sujet ; par curiosité, les *hackers* éthiques tentent de comprendre le fonctionnement d'un certain nombre de systèmes. Attention ! Je les distingue bien des cybercriminels. Les *hackers* que je connais n'ont jamais perturbé un système d'information. Certains se sont amusés à cracker la sécurité de la console Nintendo ; j'en connais même un qui a été invité au Japon afin qu'il explique comment il avait procédé. Ce sont des gens qui font cela par *hobby*, voire par souci de reconnaissance. On retrouve toutes les strates de la pyramide de Maslow. Les contacts que j'ai dans ces milieux m'autorisent à dire que leurs actions sont très positives pour comprendre les problématiques auxquelles nous sommes confrontés.

Combien d'entreprises ont-elles clairement établi une séparation entre ce à quoi a accès l'administrateur réseau et l'ensemble du trafic des données de l'entreprise ? Parfois, on ne voit pas les problèmes immédiats qui pourraient être facilement réglés. C'est pourquoi il est utile pour notre information que des garde-fous existent, en l'occurrence des gens à même de signaler des failles que nous n'aurions pas été capables de détecter et que les constructeurs n'ont aucun intérêt à divulguer. Aujourd'hui, les choses sont tellement complexes qu'une entreprise ne peut pas garantir au-delà d'un certain temps la sécurité des produits qu'elle vend. Le développement d'un produit mobilise des dizaines de personnes, qui mettent leur savoir en relation avec celui de milliers d'autres personnes sur Internet. Parmi elles, certaines s'amuseront à cracker ce produit. La sécurité étant quelque chose de dynamique et d'évolutif, elle doit toujours être remise en cause.

Christophe Naudin. Pour ma part, je ne travaille pas avec les *hackers* et je n'établis aucune distinction entre eux ; pour moi, ils sont tous gris, si j'ose dire : on ne sait jamais s'ils vont récidiver. Ces propos n'engagent que moi ! Ceux que j'ai rencontrés, qui m'assuraient être capables de cracker la puce du passeport biométrique français, ce qui m'intéresse au premier chef, n'ont jamais réussi à passer des paroles aux actes. On dit que la recette est disponible sur les forums de discussion. J'attends de voir, mais, pour le moment, je n'ai rien vu.

Je reviens sur les propos très intéressants de M. Koch. La faille, c'est l'homme. Même si l'on arrive à sécuriser 99,99 périodes, il restera toujours une faille, la faille humaine. Il faut l'accepter, car nous sommes dans une société d'humains. Ou alors nous devenons une société de robots. Tout cela n'annonce-t-il pas la disparition de l'informatique ? C'est la thèse de Michel Riguidel, qui pense que nous sommes à la fin de l'ère informatique. Soit, mais alors j'ignore comment je travaillerai dans deux ans, dans trois ans. Sans l'informatique, je ne sais plus rien faire !

Gwendal Le Grand. Sommes-nous à la fin de l'ère d'Internet ? Je ne le pense pas. Au contraire, je pense que nous en sommes plutôt au début. Certainement évoluera-t-il et sera-t-il confronté à des problèmes inhérents à sa conception. Initialement, il était conçu comme un outil simple, non sécurisé ; par la suite, il a pris une très grande ampleur. Aujourd'hui, il fait l'objet d'une utilisation de plus en plus massive.

L'arrivée du haut débit chez les particuliers a été une révolution. Dès lors, les utilisateurs, après avoir été des consommateurs de contenus, sont devenus des producteurs de contenus. On utilise l'informatique tous les jours sur un plan professionnel. Demain, la révolution, ce sera l'Internet des objets : les objets seront eux-mêmes directement connectés à Internet. Cela aura une très grande utilité quant à la traçabilité des produits, mais de nouveau risques apparaîtront en termes de protection des données personnelles. Aussi, je ne crois pas du tout à la fin d'Internet. En revanche, il est clair qu'Internet connaîtra de profondes mutations, notamment des changements d'usage. Cela créera de nouveaux enjeux, parce que tous les objets de votre environnement ambiant pourront détecter votre présence et échanger avec l'extérieur, à votre insu, un certain nombre de données. Les enjeux en termes de contrôle sont très importants pour une autorité comme la CNIL.

Quant aux hackers, nous exerçons une veille avec les moyens dont nous disposons. Nous recevons également des plaintes. Dans certains cas, des citoyens signalent à la CNIL un certain nombre d'événements sur la base desquels nous pouvons être amenés à déclencher des missions de contrôle. Nous avons donc des contacts avec les citoyens au sens large par le biais de ces signalements.

Enfin, pour combattre la cybercriminalité, la CNIL exige, dans toute opération de traitement de grande ampleur, la mise en place de mesures de sécurité – chiffrage, authentification sur les sites – visant à rendre plus difficiles toute possibilité de fraude et toute usurpation d'identité. Nous sommes également consultés dans le cadre de la mise en œuvre de traitements à l'échelle nationale, comme par exemple la mise en place du passeport biométrique et l'accès aux bases biométriques utilisées par ce système. Dans ce contexte, nous avons par exemple demandé que la sécurité de la puce contenue dans ce passeport soit correctement évaluée.

Question. Je veux bien comprendre votre raisonnement intellectuel sur la position de la CNIL et sur les fichiers positifs. Le problème, c'est que la France n'est pas isolée et qu'elle ne peut pas rester à l'écart de ce qui se passe dans les autres pays d'Europe. Existe-t-il un projet de CNIL européenne ? Si tel était le cas, cela simplifierait les choses. Je pense aussi à la directive – ou au projet de directive – sur les moyens de paiement.

Gwendal Le Grand. Il n'existe pas de projet de CNIL européenne en tant que telle. Peut-être la situation évoluera-t-elle l'année prochaine quand sera sans doute lancé le chantier de révision de la directive générale sur la protection des données. Chaque pays membre de l'Union européenne dispose d'une autorité de protection des données équivalente à la CNIL, chacune d'entre elles agissant à un échelon national. Toutes ne sont pas dotées des mêmes pouvoirs, même si toutes fondent leur action sur une règle issue de la transposition de la directive en droit national. En France, il s'agit de la loi « informatique et libertés ». Néanmoins, tous les deux mois se réunissent au G29 à Bruxelles, en séance plénière, les responsables des équivalents européens de la CNIL.

Le but de ces réunions est d'harmoniser l'application de la directive sur la protection des données. Tout à l'heure, j'ai pris l'exemple des moteurs de recherche, au sujet desquels un avis sur l'interprétation du cadre législatif européen auquel ils doivent être soumis, a été adopté à l'unanimité.

Cette réflexion s'applique à un certain nombre de secteurs comme celui des réseaux sociaux, pour lesquels un avis est en cours de préparation. Dans un certain nombre de domaines, nous sommes parvenus à une vision commune. Le G29 a donc un rôle consultatif alors que le réel pouvoir est détenu, au niveau national, par les autorités. Certes, ce comité n'a pas de pouvoir de contrôle et de sanction, contrairement aux commissions nationales, mais, bien évidemment, chaque pays tient compte des positions européennes lorsqu'il s'agit d'appliquer la loi nationale.

En résumé, il n'existe pas une « super CNIL » européenne, mais les CNIL européennes se réunissent régulièrement pour harmoniser certaines positions.

Question. Vous établissez une distinction entre le *hacker* éthique et le pirate. La loi française établit-elle une telle distinction ? Je pense à cette personne qui avait cracké l'algorithme de la carte bancaire. Voilà deux jours, j'ai lu dans la presse qu'un certain Chris Paget avait réussi à pirater le passeport américain pendant 20 minutes.

Myriam Quéméner. La loi française n'établit aucunement une telle distinction. Elle ne donne aucune définition précise de ce qu'est un pirate. Ce sont les investigations qui sont menées dans le cadre de l'enquête qui permettront de savoir si on a affaire à un étudiant en informatique, qui n'agit que dans le but de tester les systèmes, ou à quelqu'un qui relève de la criminalité organisée. Ces éléments de l'enquête détermineront s'il s'agit d'un acte individuel ou d'un acte s'inscrivant dans un réseau.

Question. On pourrait imaginer qu'un réseau de cartes bancaires ou Nintendo portent plainte contre un *hacker* qui, sans être malintentionné, mettrait au jour une faille qui pourrait être lourde de conséquences pour l'activité commerciale de l'entreprise.

Christophe Naudin. Le cas s'est déjà produit et le réseau carte bleue a déjà porté plainte contre des gens. Il ne leur reprochait pas tant d'avoir rendu publique cette faille que, comme toute entreprise extrêmement soucieuse de sa communication, d'avoir porté atteinte à son image. Assez bêtement, il a fait condamner un informaticien qui avait réussi à mettre au jour une faille, plutôt que d'intégrer ses remarques dans le processus de fabrication des cartes.

Stéphane Koch. Soyons réalistes ! Si une faille devient « publique », cela signifie qu'elle a déjà prospéré. Ce qu'on appelle les failles Oday, c'est-à-dire les failles du jour, sont vendues dans les milieux cybercriminels. Va-t-on nous empêcher d'avoir connaissance d'une faille de sécurité alors que tous les cybercriminels sont déjà au courant depuis des lustres ? C'est une aberration ! Il faut arrêter de croire que seules les entreprises disposent de compétences : celles-ci sont, heureusement ou malheureusement, partagées. N'oublions pas que la conjoncture économique a mis sur le marché un certain nombre de compétences, un certain nombre de personnes qui n'ont d'autre objectif que de trouver des moyens de subsistance.

Je vous conseille la lecture du numéro de janvier-février du magazine *Misk* , qui a consacré un dossier très intéressant à la cybercriminalité. Il y est mentionné que, en 2006, en Russie, un informaticien sur dix était au chômage. Dans ces conditions, il faut bien se débrouiller pour trouver des moyens de subsistance !

Ces gens-là ne vont pas toujours savoir s'imposer des règles morales, surtout dans des pays qui, pour être économiquement défavorisés, disposent néanmoins de compétences de très haut niveau. Il faut donc tenir compte de cette asymétrie économique et comprendre la manière dont on voit la sécurité. Dans la mesure où l'on ne peut pas tout sécuriser, fabriquons un produit qui puisse trouver sa place dans cette zone tampon.

Reprenons l'exemple du passeport biométrique. Il faut partir du principe qu'il ne peut être entièrement sécurisé. Un système de bases de données contiendra les empreintes d'origine contenues dans ces passeports biométriques. Le problème, à ce jour, c'est que tous les pays européens n'ont pas adhéré à ce système de bases de données, ce qui rend impossible tout double contrôle, ce qui empêche de savoir si un passeport a été modifié ou non. Si tout le monde adhère à ce système, la recherche d'une modification éventuelle du passeport n'est plus prioritaire dans la mesure où celle-ci peut être détectée.

On ne peut pas tout sécuriser. Dans ces conditions, il faut se demander ce que l'on peut faire. Par exemple, on doit avoir une réflexion sur les accès distants aux entreprises. Certaines entreprises sont ultra-sécurisées ; elles sont équipées de systèmes d'alerte, de contrôle ou d'alarme, avec identification par empreintes biométriques pour accéder aux locaux. Dans le même temps, il est possible, avec un *laptop*, de chez soi, d'accéder à distance, par canal sécurisé, à l'entreprise. Il suffit de connaître les codes, qu'on peut, si nécessaire, obtenir sous la contrainte auprès de salariés.

Je me rappelle être allé une fois chez un spécialiste parisien de l'intelligence économique. Traitant des dossiers très sensibles depuis son appartement, il était fier de me montrer les systèmes de sécurité dont étaient dotés ses ordinateurs. Je lui ai démontré qu'il faudrait moins de cinq minutes à quiconque pour s'introduire dans son appartement et emporter son ordinateur, sans que la police ait le temps d'intervenir.

Il faut donc mener une réflexion globale, en partant du principe que tout ne peut pas être sécurisé. Les connaissances sont telles que ce qui est sécurisé aujourd'hui ne le sera plus demain.

Je citerai le cas de la société Kudelski, une société suisse spécialisée dans le cryptage des signaux de télévision payante, qui travaille notamment avec Canal+. Un procès l'a opposée à la société NDS, filiale du groupe Murdoch, après que celle-ci a réussi indirectement à cracker les systèmes de protection de la carte à puce utilisée par les terminaux de la chaîne cryptée. Comment a-t-elle fait ? Aux États-Unis, aux termes du *Digital Millenium Copyright Act*, le DMCA, il est interdit d'étudier un produit, de le décomposer, de le démonter afin de connaître son mode de fonctionnement. Cette loi est la manifestation, en quelque sorte, d'une forme de protectionnisme. Du coup, la société NDS a utilisé sa filiale israélienne, qui disposait d'un certain nombre de spécialistes du cryptage. Ils ont invité un ancien *hacker*, qui leur a dispensé un cours sur la carte de Canal+ et qui leur a expliqué comment il était possible d'exploiter l'une de ses failles de sécurité. Après, comme par hasard, on a retrouvé sur Internet la solution pour contourner cette sécurité et de fausses cartes ont été produites.

Il s'agit là d'un nouveau type de concurrence déloyale, qui recourt à différents biais juridiques pour prospérer. Les cybercriminels – notez bien que je n'assimile pas cette société aux cybercriminels – savent mieux que quiconque utiliser la loi et la contourner, si besoin en utilisant les différences de législation entre les pays.

Myriam Quéméner. Je suis tout à fait d'accord avec vous. Les cyberdélinquants suivent de très près les décisions judiciaires et adaptent leurs actions en fonction des condamnations prononcées.

Question. Pour en revenir à l'usurpation d'identité sur Internet, on avait entendu parler d'une carte nationale d'identité électronique. L'idée a-t-elle été complètement enterrée ? Ou bien le projet est-il toujours envisagé, sachant que, si elle devait un jour sortir, cette carte d'identité serait crackable au bout de six mois ou de trois ans ?

Christophe Naudin. Vous faites référence au projet de carte nationale d'identité électronique, qui avait été lancé avant l'élection présidentielle. Il existe toujours. Il est vrai qu'il fallait préalablement expérimenter les documents électroniques sur des échantillons réduits de population. Deux tentatives ont été menées. Vous avez sans doute entendu parler de l'amendement Mariani, relatif au rapprochement familial, qui visait à autoriser les prélèvements d'ADN sur une population estimée à environ 3 000 individus. Sur un plan biométrique, les dispositions contenues dans cet amendement étaient très intéressantes, mais celui-ci, pour des raisons politiques, n'a pas vraiment connu de suite. La carte nationale d'identité électronique, quant à elle, concerne environ 30 millions de personnes en France. Quant aux titres de séjour, on pourrait envisager de les numériser ou d'y introduire des données biométriques, mais vous imaginez quelles réactions pourrait susciter une telle décision.

C'est pourquoi il a été décidé de travailler sur un document qui est peu utilisé et peu répandu en France : le passeport.

Dans un premier temps est apparu le passeport électronique, équipé de la fameuse puce dont Stéphane

Koch parlait tout à l'heure. Sans doute contient-il quelques failles, mais entre le passeport version Delphine II, que vous possédez sans doute actuellement, le passeport électronique, qui a commencé d'être délivré, et le passeport biométrique, qui sera délivré à compter d'octobre prochain, il existe un gigantesque *gap* en termes de protection.

A ce jour, je n'ai encore jamais vu un passeport électronique contrefait. Je ne dis pas qu'il n'est pas possible de le falsifier, mais je puis vous dire qu'il est beaucoup plus sécurisé que les anciens passeports. Même si je ne suis pas neutre en la matière, je puis vous dire que vous n'avez aucune raison de ne pas avoir confiance, car l'État a très bien travaillé sur ce dossier. Nous allons mettre en place très rapidement les passeports biométriques en pratiquant des essais aux frontières. Car ce qui nous intéresse, c'est la capacité de contrôle.
Quand le passeport biométrique sera bien au point, je pense qu'on passera à la carte nationale d'identité électronique, qui concerne 30 millions de personnes. Aujourd'hui, moins de 5 millions de personnes détiennent un passeport.

Question. Je précise ma question : sur le plan professionnel, ce qui m'intéresse, c'est d'utiliser un document de l'État pour identifier et authentifier mes clients sur Internet.

Christophe Naudin. C'est la question de la signature électronique. M. Le Grand répondra certainement mieux que moi à cette question. La question essentielle, c'est de savoir si l'on autorise des sociétés commerciales telles que la Caisse d'épargne à disposer d'un certain nombre de clés lui permettant non pas d'identifier un document, mais d'authentifier sa validité.

Gwendal Le Grand. Il faut bien faire la distinction entre les fonctionnalités qui sont offertes par le passeport biométrique, qui sera rendu obligatoire à partir de juin 2009 – une puce qui contient vos données d'état civil et vos empreintes digitales – et la carte d'identité électronique, à laquelle monsieur a fait référence, qui offrirait en plus la possibilité d'accéder aux e-services de l'administration ou du privé.
Je ne peux guère vous préciser le calendrier. Il s'agit d'un projet que nous avons vu et revu à plusieurs reprises, dont il a été annoncé de multiples fois qu'il serait relancé en 2009.
A la fin de l'année 2007, l'AFNOR a rendu public un rapport sur les usages qui pourraient être faits de cette carte d'identité électronique. Il était question de disposer d'une carte dotée de biométrie et pouvant être utilisée pour les e-services.

Toutefois l'authentification biométrique serait exclusivement réservée aux forces de police et gendarmerie sans qu'il soit possible d'y recourir dans le cadre des télé-procédures, qu'elles soient publiques ou privées. Dans le cadre des téléprocédures, la carte pourrait donc servir de vecteur d'authentification auprès des banques par exemple.

Dans son étude, l'AFNOR recense les utilisations qui pourraient être faites de la carte d'identité électronique dans le domaine des téléprocédures au sens large. Évidemment, un certain nombre d'acteurs poussent pour que cette fonctionnalité de téléservices soit mise en place dans la mesure où elle pourrait être extrêmement utile pour sécuriser les données sur Internet puisqu'elle permet à une personne de s'authentifier et de signer des documents d'une manière beaucoup plus sûre qu'actuellement.

Je ne peux guère vous en dire plus sur le calendrier, mais, de toute façon, ce projet devrait être examiné par le Parlement.

Stéphane Koch. En Suisse, depuis 2005, la signature électronique a légalement la même valeur que la signature manuscrite. Mais, concrètement, il faut faire attention à ne pas dissocier le comportement de l'homme, sa culture, des technologies qu'on met en place. Le pas sociologique est largement plus important que le pas technologique. Pour sensibiliser les gens à ces signatures électroniques, pour qu'ils les adoptent, du temps et de l'argent seront nécessaires. Aujourd'hui, mettre sur le marché un produit que les gens ne comprennent pas, c'est ouvrir la porte à sa falsification à grande échelle. Ce produit restera sécurisé, mais de faux produits circuleront ou des gens usurperont ces certificats d'utilisation. Aussi, nous n'aurons pas atteint notre objectif. C'est pourquoi les gouvernements et les acteurs économiques doivent vraiment sensibiliser les gens et leur faire comprendre comment l'on gère cette problématique. Et il y a du travail ! Voyez la gestion des méls !

Marie Bazetoux. Je sais qu'il reste encore quelques questions, mais nous avons pour habitude d'essayer de respecter notre programme.

Guy, je crois que tu voulais dire quelques mots avant la conclusion de cette table ronde.

Guy de Felcourt. Je voudrais en effet revenir sur deux ou trois choses importantes qui ont été dites au cours de cette table ronde.

Va-t-on vers une économie Internet ? La réponse est clairement positive. Vous connaissez le plan numérique 2012. L'économie numérique est très importante pour le Gouvernement, pour la France. Pour en avoir parlé récemment avec des parlementaires, je peux vous dire qu'il y aura une forte mobilisation sur ce sujet.

De même, nous disposerons tôt ou tard d'un système d'identification ou d'un système d'authentification. Après, toute la difficulté est de savoir combien de millions de consommateurs et quelle frange de mes clients seront concernés. On entre là dans des considérations plus commerciales. Il faut prévoir des solutions pour plusieurs types de clients, pour plusieurs technologies, qui soient justement ouvertes non seulement en termes de technologie, mais aussi en termes de services et d'accompagnement.

Tout à l'heure, on a parlé de spams, de SMS frauduleux incitant à rappeler des numéros surtaxés. Des réponses existent, mais toute la difficulté pour les consommateurs consiste à trouver ces réponses. Les problèmes que vous rencontrez, vos clients les rencontrent également. Nous avons prévu des réponses spécifiques en termes de service au client pour qu'il puisse rapidement surmonter ce genre de difficultés.

Je retiens de ce qui a été dit au cours de cette table ronde, que nous sommes confrontés à un double défi : celui de protéger nos données personnelles en tant qu'individu et celui de gérer notre identité. C'est un processus probablement plus long et plus complexe qu'on ne l'imagine et certainement encore plus difficile pour vos clients et pour les consommateurs. De manière responsable, nous avons à cœur de pouvoir aider vos clients consommateurs à faire face et à trouver les bonnes réponses à ces problématiques, qui ne sont pas les problématiques d'un moment, mais celles de la prochaine décennie.

Gras Savoye et CPP France, compte tenu de leur expérience et de leur savoir-faire, sont là pour vous aider dans cette démarche.

Marie Bazetoux. Les Tables Rondes de Gras Savoye font systématiquement l'objet d'une retranscription. Celle-ci vous sera adressée dès que possible. Merci de songer à nous laisser vos coordonnées en quittant la salle.

Je tiens à remercier l'équipe qui a travaillé plusieurs mois sur cette table ronde avec enthousiasme et sérieux.

Je vous remercie d'avoir été aussi nombreux et aussi attentifs. A titre personnel, je me suis sentie très concernée. Je me doutais qu'il existait des risques ; à présent, j'en suis convaincue. Je ne pense pas qu'il s'agisse de fantasmes ; les risques sont bien réels. Nous avons tenté de vous démontrer que ce type de raisonnement et de fonctionnement était au cœur de notre vocation de spécialistes de l'ingénierie. C'est ainsi que nous entendons travailler avec vous : aborder les problématiques sociétales de comportements, de risques, et définir les moyens de prévenir, d'informer et, peut-être, de rassurer.

Nous vous donnons rendez-vous à notre prochaine Table Ronde.

ANNEXES